THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on Internet and Communications Resilience

November 16, 2017

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Automated and distributed attacks facilitated through botnets threaten the security and resiliency of the Internet ecosystem and the Nation's critical infrastructure. The size and scale of Distributed Denial of Service (DDoS) attacks facilitated through botnets has risen dramatically in the past few years. This development increases concern that such attacks could overwhelm the United States (U.S.) critical infrastructure. Further compounding the problem, the growing mix of Internet of Things (IoT) devices provides a ripe environment for malicious actors to launch global automated attacks using compromised IoT devices. This situation threatens the security of the Internet ecosystem.

In May 2017, the Executive Office of the President (EOP) requested that the President's National Security Telecommunications Advisory Committee (NSTAC) examine how the private sector and government could improve the resilience of the Internet and communications ecosystem.[1] The EOP, in support of Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, specifically asked the NSTAC to identify ways to encourage collaboration to reduce the threats from automated and distributed attacks (for example, botnets). This *NSTAC Report to the President on Internet and Communication Resilience* ("Report") presents the NSTAC's work and its recommendations.

KEY LESSONS LEARNED

A greater sense of urgency is required. The threat will only increase as the number and type of IoT devices grow and as such devices become more autonomous, capable and ubiquitous. Wherever possible, studying, testing, and implementing possible solutions should be carried out in parallel rather than sequentially. Efforts must be made to get ahead of the threats.

Public-private partnerships are key. Public-private partnerships, such as the Financial Systemic Analysis & Resilience Center, as well as efforts by the Federal Bureau of Investigation, Microsoft, and Internet Service Providers (ISPs), show that criminal botnets and command and control structures can be effectively disrupted. Collaboration between the public and private sectors is vital to mitigating botnets.

Solutions depend on every part of the Internet ecosystem. Distributed attacks are a complex challenge. No single segment of the Internet ecosystem can solve this issue alone.

Solutions depend on both standards and innovation at the network and Internet infrastructure layer. While a variety of standards and best practices exist, there is a lack of global consistency in the adoption of these practices. Standards play a vital role in securing the Internet ecosystem, however, with a fractured standards environment and many devices manufactured outside the U.S., standards deployment will likely be uneven. There is a need for emerging solutions at the infrastructure layer. Further, there may be value in developing standards upstream from the device, such as at the chipset level.

[1] White House Office of the Press Secretary. *Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. May 16, 2017. https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

Education and awareness lag. The Nation needs an informed digital citizenry. Individuals and enterprises must understand how their decisions impact networks, systems, and each other.

Unclear international norms complicate challenges. Much of the threat comes from overseas, so international investigations and prosecutions are critical. Global cooperation is needed on technical standards, device security, attribution, traffic flows, and shared norms and defenses.

A new trust model is needed. Transmission Control Protocol/Internet Protocol, Border Gateway Protocol, the Domain Name System, and many other protocols that underlie the Internet were not designed with security as a primary concern. As networks become more open and interconnected, this trust model can no longer be the sole foundation for Internet security.[2] Defining how greater trust can be built into the Internet should be a key focal point of the cybersecurity Moonshot effort described below.

KEY RECOMMENDATIONS

The Private Sector Must Act. Addressing automated and distributed attacks requires vigilance across the Internet ecosystem including network service providers or ISPs, device manufacturers, software developers, cloud, application and hosting providers and other entities, all of which comprise the Internet infrastructure. The NSTAC recommends the following short-term actions:

- **Accelerate adoption of security guidelines**. The Communications Sector should collaborate with the Department of Homeland Security (DHS), as the Sector Specific Agency for Communications, and the National Telecommunications and Information Administration (NTIA) to identify relevant common security practices for communications networks to protect against botnets and DDoS attacks in domestic and global standards bodies (e.g., Best Common Practice (BCP) 38) and identify barriers to adoption and/or incentives to promote adoption. Networks may not be limited to large Internet Service Providers (ISPs) as many practices should be deployed by any entity running a publicly addressable network including enterprise businesses.

- **Develop IoT device security guidelines.** The Department of Commerce (DOC) through the NTIA and the National Institute of Standards and Technology (NIST) should work with device makers to facilitate the development of a baseline of recommended common sense security practices consistent with the risk associated with a device. DOC should also review the role and viability of voluntary device certification and independent testing to ensure device security.

- **Continue to innovate around infrastructure-based solutions.** Government and industry cannot rely solely upon the consistent adoption of standards to secure IoT. ISPs, wireless service providers, router manufacturers, security solutions providers, and others are developing services to manage IoT security. These solutions can be employed at different layers of the network from inside the home (e.g., Ethernet, Wi-Fi) to include; Long Term

[2] Communications Security Reliability and Interoperability Council (CSRIC) V: Working Group 10, Legacy Risk Reductions (2017) (Legacy Risk Reductions Report), https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf.

Evolution or Fifth Generation wireless network infrastructure; the Multiprotocol Label Switching network core; and at the application layer or in the cloud. [3] These capabilities are emerging and the private sector should continue to invest in these technologies. The U.S. Government should help drive these capabilities by incorporating them in federal procurement requirements and raising awareness of their application for IoT security.

- **Promote enterprise security controls to improve IoT device security.** NIST should develop use cases building upon the NIST Cybersecurity Framework for enterprises to incorporate IoT into risk management. Many IoT devices will serve a dual purpose in both consumer and enterprise networks. Enterprises and the government can promote IoT security standards for devices in purchasing arrangements.

- **Promote software assurance.** The software industry should work with DHS to promote common practices for software assurance. Awareness of best practices would provide buyers visibility into how their suppliers incorporate security and help them make better procurement decisions.

The Government Must Act. The government should respond to the growing threat from botnets in three fundamental areas. The NSTAC recommends that the government (1) take greater actions to support law enforcement; (2) promote the adoption of security standards and best practices; and (3) develop an effective international cybersecurity strategy.

- **Enforcement**

    - **Support public-private collaboration and takedowns.** The government, including the Department of Justice (DOJ), should increase takedown efforts that have successfully mitigated the impact of botnets. The U.S. Government should increase incentives, particularly within DOJ, to make preventing cybercrime and disrupting botnets a higher priority. The national security implications of botnets justify prevention as well as prosecution. The DOJ may need additional resources in order to increase these efforts which also are dependent upon collaboration with both the private sector and potential international partners.

- **Promoting Adoption of Security Standards and Best Practices**

    - **Promote flexible standards using incentives and remove barriers to adoption.** NTIA, NIST, and other agencies should convene stakeholders and promote coordination across sectors to develop common standards and promote consistent practices in government and across critical infrastructure. The government should identify gaps and incentives to motivate industry to adopt standards and practices. Some industries, if lagging, may need more incentives, particularly when it comes to mitigating risks of devices currently in place. Smaller businesses may also lack the same resources and access to cyber expertise as larger entities. Finally, the insurance market may drive

[3] Cisco offers an example framework for IoT security at each layer of the network at https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html

improvement as underwriters probe companies on the maturity of their security risk management practices and offer lower premiums to companies higher on the maturity scale.

- **Seek to harmonize security requirements at the federal, state, and international levels.** Cybersecurity standards, practices, and regulations are often approached in a fragmented, somewhat ineffective manner. Domestically, some states establish state-specific security requirements. Internationally, the European Union, Japan, China, and several other countries are looking at developing IoT device certification and testing programs. The U.S. Government must champion consistent interoperable IoT security standards abroad and nationally among states to encourage a unified approach.

- **Enhance government cybersecurity.** The U.S. Government should set an example by improving the security of federal networks. Information technology (IT) modernization is a key component to improving federal cybersecurity. The government should use its ongoing efforts to modernize federal IT to drive adoption of new technologies and security solutions in the private sector.

- **International Cybersecurity**

  - **Develop a comprehensive U.S. standards engagement strategy**. The United States has traditionally relied upon collaboration with private industry to enhance the government's efforts in international standards forums. However, in recent years foreign entities have rapidly increased their presence in shaping international standards. The U.S. Government should collaborate with the private sector to ensure representation in key forums impacting the development of technology standards that may lead to national security concerns in the future.

  - **Develop an effective international cybersecurity strategy focused on raising the cost to attackers.** The government should prioritize the development of a comprehensive international cybersecurity strategy leveraging traditional diplomatic tools and support for global law enforcement with the objective of raising the costs to cyber attackers. Many DDoS attacks are international, and the government must implement a global strategy to address the threats. The persistent nature of cyber attacks means that even entities with the best practices can still be exploited. The Nation must raise the cost for attackers while at the same time adopt standards, practices, and new innovative technology solutions to make attacks more difficult.

- **The Nation Needs a Cybersecurity Moonshot.** A future NSTAC effort should analyze the concept of launching a cybersecurity Moonshot in two phases. The first phase would review other successful Moonshot models, including outside of the cybersecurity domain, to identify consistent principles that can be applied to the cybersecurity challenge. As a starting point, this would include studying models that feature at least the following characteristics:

  - National Call to Action;
  - Focus on an End Goal, setting a specific objective or end state by a certain date; and
  - A Government-led Multi-Stakeholder Process.

In the second phase of study, the NSTAC would seek to clarify key cybersecurity considerations related to the identified Moonshot principles (Call to Action, End-Goal Focus, and Multi-Stakeholder Process), drawing on cybersecurity experts to define an end goal and sub-elements, and expanding on material the NSTAC reviewed while preparing this Report.[4]

[4] One example was the briefing on Unified Memory Reference Models provided by Steve Wallach. Micron Technology, Inc. *Briefing to the NSTAC ICR Subcommittee*. September 7, 2017.

1.0 INTRODUCTION

There is growing concern about the potential for malicious actors to use botnets to facilitate large scale Distributed Denial of Service (DDoS) attacks that could disrupt U.S. critical infrastructure. Attackers exploit fundamental Internet vulnerabilities such as Domain Name System (DNS), Network Time Protocol (NTP), Simple Service Discovery Protocol, Character Generator Protocol (CharGen), and other protocols – to dramatically increase the size and scale of attacks.[5] Further, while botnets are not new, Internet of Things (IoT) devices compound the risk as they are connecting an increasing number of people, devices, and networks. The Mirai botnet attack in 2016 was the first IoT-based botnet with a significant impact, but such attacks are expected to rise.[6] These factors have led to a rapid increase in the size and scale of DDoS attacks. For example, according to one source, attack sizes ranged around 100 Gigabits per second (Gbps) until mid-2012, after which the size began to dramatically increase. The same source estimated the peak attack size in 2016 to be approximately 800 Gbps, an eightfold increase over the past 4 years.[7] This Report provides recommendations to reduce the potential impact of botnets and DDoS attacks and threat they pose to the Nation's critical infrastructure.

1.1 Scoping and Charge

In May 2017, the Executive Office of the President (EOP) requested that the President's National Security Telecommunications Advisory Committee (NSTAC) examine how the private sector and government can collaborate to improve the resilience of the Internet and communications ecosystem.[8] The EOP, in support of Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, tasked the NSTAC with identifying ways to encourage collaboration to reduce threats from automated and distributed attacks (such as botnets). Additionally, the EOP asked the NSTAC to consider what rules of engagement will enable cooperative efforts to protect the Nation's cybersecurity posture. In June 2017, the NSTAC formed the Internet and Communications Resilience (ICR) committee to address the EOP's requests.[9] The EOP stated that the NSTAC's findings would inform a preliminary report to be issued by the Department of Commerce (DOC) and the Department of Homeland Security (DHS) in January 2018.

DDoS and botnet attacks are of increasing concern. In 2014, the NSTAC observed that "[b]y 2020, there will be tens of billions of devices in use. Now is the time to influence how those devices are designed and what protocols govern their use; after they are deployed, new policy

[5] Arbor Networks Worldwide Infrastructure Security Report, Volume XII, available at https://www.arbornetworks.com/insight-into-the-global-threat-landscape

[6] See Computer Weekly, "Global Hacker Botnet Tops 6 Million Hijacked Devices", September 27, 2017 http://www.computerweekly.com/news/450427023/Global-hacker-botnet-tops-6-million-hijacked-devices

[7] Arbor Networks Worldwide Infrastructure Security Report Volume XII, available at https://www.arbornetworks.com/insight-into-the-global-threat-landscape

[8] White House Office of the Press Secretary. *Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. May 11, 2017. https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

[9] A report from the ICR Subcommittee is due in October 2017. DHS and DOC will release a preliminary report by January 2018 and a final report by May 2018.

will only affect change at the margins."[10] The NSTAC's goal is to help the Administration deepen government and private cooperation.

This *NSTAC Report to the President on Internet and Communication Resilience* ("Report") presents the NSTAC's work and its recommendations. It provides the EOP with an actionable roadmap for addressing the threats posed by botnets and other distributed and automated attacks on our Internet infrastructure, online services, and end-users. This Report examines threats and solutions, from short-term remedies to long-term Internet architecture development. The Report is organized as follows:

- Section 1 explains scoping and goals.
- Section 2 describes the global Internet ecosystem and how distributed attacks threaten the security of an increasingly connected world.
- Section 3 identifies challenges and mitigation efforts in each segment of the ecosystem: networks, consumers/edge/devices, enterprise, and software/applications/operating systems (OS).
- Section 4 offers short- and long-term recommendations, as well as a follow-on Moonshot study to holistically address cybersecurity challenges more generally, including automated and distributed attacks.
- Section 5 identifies opportunities for the government to use the unique tools available to it and collaborate with the private sector.

1.2 Approach

The NSTAC utilized several methods to gather information, including briefings from subject matter experts, conducting policy reviews, and examining cybersecurity threat reports, articles and best practices to combat these threats. Among other things, the NSTAC:

- Received over two dozen briefings from experts across industry, academia, and the public sector, as reflected in Appendix A;
- Reviewed private and Federal Government cybersecurity policies, regulations, reports, and best practices, such as the National Institute of Standards and Technology's (NIST) Cybersecurity Framework;
- Reviewed current industry cybersecurity best practices and research; and

[10] President's National Security Telecommunications Advisory Committee (NSTAC). *NSTAC Report to the President on the Internet of Things*. November 19, 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf. Appendix E, E-5.

- Examined studies and comments about cybersecurity at NIST and National Telecommunications and Information Administration (NTIA).

The NSTAC examined weaknesses in ecosystem security and identified areas to improve security at the network, device, and user levels. In this Report, the NSTAC recommends steps to create a more secure Internet ecosystem, focusing on government and industry partnerships to address malicious activity.

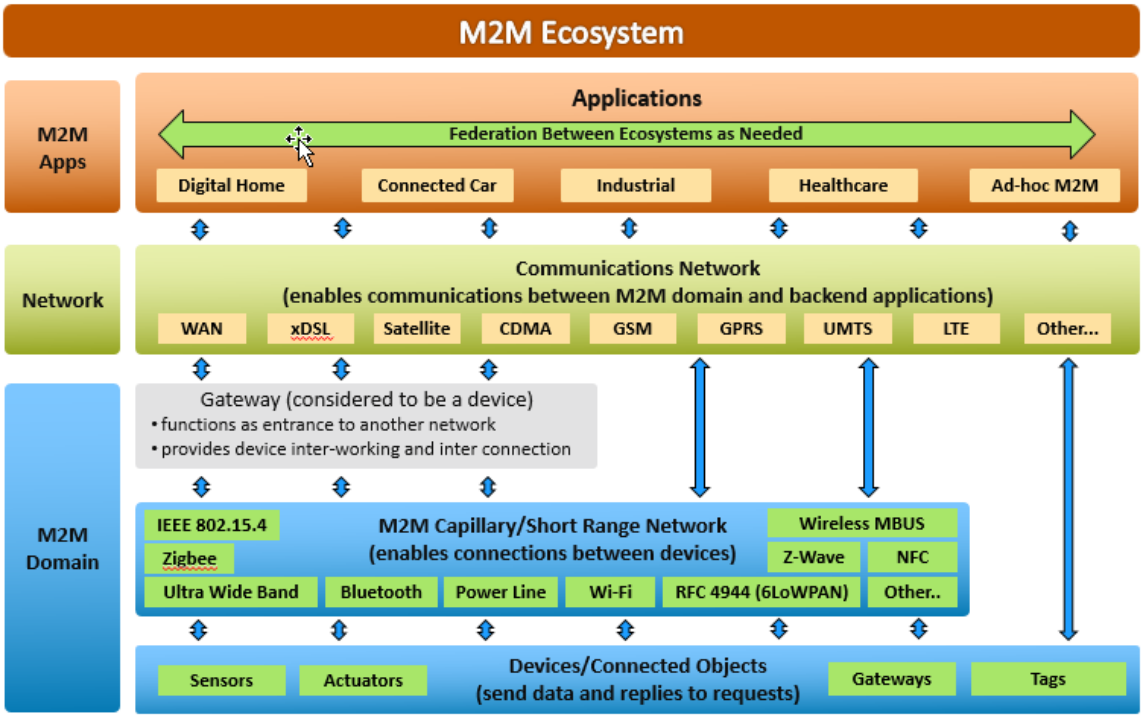
2.0 THE GLOBAL NATURE OF THE ECOSYSTEM FACILITATES DISTRIBUTED, AUTOMATED ATTACKS

The Internet ecosystem is diverse and diffuse, and each part plays a role in security. The ecosystem continues to grow with a proliferation of devices that link everyday items such as cars and thermostats to the Internet, support industrial control systems, and monitor critical infrastructure. A malicious actor controlling an infected device creates multiple risks. First, the device could be used in a denial-of-service attack on another device. Second, bot software on a device could be used to steal information from, or track, the device. For example, bot software on a Congressperson's in-car navigation software could track the vehicle's movements. Third, bot software on a device could be used to generate a denial of service (DoS) event on the device itself. Fourth, the bot could manipulate data or cause incorrect device behavior, thereby endangering the safety of users or corrupting device data influencing results for data consumers. As IoT devices proliferate and serve increasingly sensitive functions, such as autonomous driving and industrial controls, incapacitating IoT devices can have significant and dangerous real-world impacts.

2.1 The Global Internet and Communications Ecosystem Is Diverse and Evolving

End users, Internet service providers (ISPs), network operators, manufacturers, and software developers comprise the global Internet ecosystem. Governments and international systems also play a role. The layers supporting machine-to-machine (M2M) IoT that compose the ecosystem are illustrated in Figure 1 on the following page.

Figure 1. The M2M Ecosystem



Source: AT&T Presentation on NSTAC Report to the President on the Internet of Things. November 19, 2014.

Although some contend ISPs are in the best position to mitigate botnet attacks, the IoT is made up of devices, transport networks, applications, and the companies and users deploying them. Each segment confronts threats and requires attention.

Figure 2. Threat Landscape

Source: Brian Rexroad. AT&T. Briefing to the NSTAC ICR Subcommittee. July 20, 2017.

Experts anticipate a migration toward managed IoT services as companies offer comprehensive solutions.[11] As IoT devices proliferate, they provide a new scale for botnets.

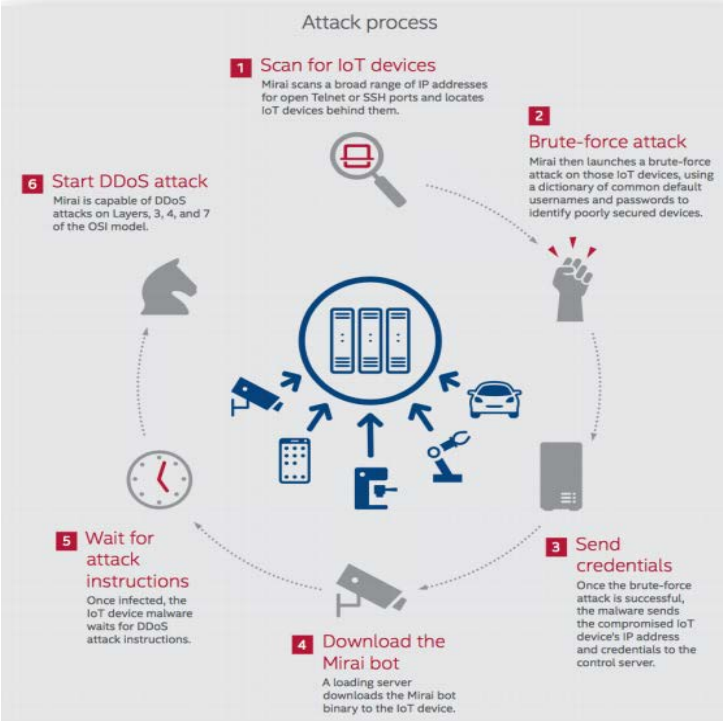
[11] Kevin Walsh. Palo Alto Networks, Inc. *Briefing to the NSTAC ICR Subcommittee*. July 18, 2017.

2.2 Botnets and Automated Distributed Attacks Evolve

Botnets were originally designed for a positive use and were subsequently repurposed for hostile actions. A bot is "a program that is installed on a system to enable that system to automatically (or semi-automatically) perform a task or set of tasks typically under the command and control of a remote administrator (a.k.a. bot master or bot herder)."[12] These programs can run code that is not provided by the vendor or authorized by its owner. Most bots can support malicious activities such as spam, phishing, click-fraud, and DDoS.

A botnet is "a network of internet-connected end-user computing devices infected with bot malware and are remotely controlled by third parties for nefarious purposes."[13] A botnet attack happens when a network of computers, IoT, or other Internet Protocol (IP)-enabled devices are commandeered to run unauthorized code in support of malicious activities such as spam, phishing, click-fraud, and DDoS. Figure 3 provides a depiction of how botnet attacks occur.

Figure 3. How Botnet Attacks Occur



Source: McAfee, https://www.mcafee.com/us/resources/misc/infographic-threats-report-mar-2017.pdf

Bots are generally delivered through infected websites or links to malicious websites embedded in phishing emails. Users may inadvertently install bots based on deceptive emails, web instructions, or via browser/OS vulnerabilities. Bots can also be deployed without any action by the end user. For example, in the Mirai botnet several devices were infected without any user

[12] Federal Communications Commission (FCC). CSRIC. III, *U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers*. March 2012. https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf.

[13] Ibid.

interaction. Default passwords for device management or vendor-installed back-doors can be compromised, permitting unauthorized access to and control of a device. Bots are also distributed via phishing schemes, spam, and other security threats. A key aspect of botnet campaigns is the persistent nature of the attacks looking to exploit any available weakness to gain access. Bots can update security patches and anti-virus software on a machine to ensure stable operation and exclusion of other bots. When people discuss botnets, they often think of DDoS attacks.[14] But botnets can facilitate data theft, illegal content distribution, processing theft, email spam, click fraud, and other attacks.[15]

Botnet attacks are increasing in size and sophistication with the rise of IoT. Some botnets use Artificial Intelligence (AI), quantum cryptography, or neuromorphic computing, to make smarter viruses that adapt at the speed of the Internet.[16] The largest attack reported was 800 Gbps, and approximately one-third of attacks peak at over 100 Gbps.[17] ISPs dramatically increased DDoS protection following the DDoS attacks on financial institutions in 2012-13,[18] but DoS attacks have increased in size, and attackers have changed tactics. For example, attackers target domains with the largest DNS record to amplify the effectiveness of their attack. Moreover, as devices become more autonomous, and include sophisticated AI, the implications for cyber malfeasance through the IoT will give rise to new and serious risks that must be anticipated and planned for in the near term.

Mitigation augments prevention. Cyberattacks will happen.[19] According to the DHS Science and Technology Directorate, 70 percent of hacking utilizes lost, stolen or weak credentials, and 60 percent of malware uses privilege escalation or stolen credentials.[20] Rather than preventing botnet attacks, experts have moved toward building more resilient networks and mitigating attacks' effects. Best practices to mitigate attacks focus on user and enterprise education about networking hygiene and vulnerability management. This includes strong authentication, turning off unwanted features, and updating services. Other mitigation tools include network and data analytics, reverse proxies, application and network firewalls and load balancers, and reconfiguring/securing Internet routers. Large-scale DDoS attack mitigation works best when complemented by datacenter/edge services. Data analytics, signals, systemic measures, anomaly detection, data sensing, and triggers are all helpful in mitigating botnet attacks. It is important to review joint characteristics and dependencies to identify similar behaviors and assign them to actors.[21]

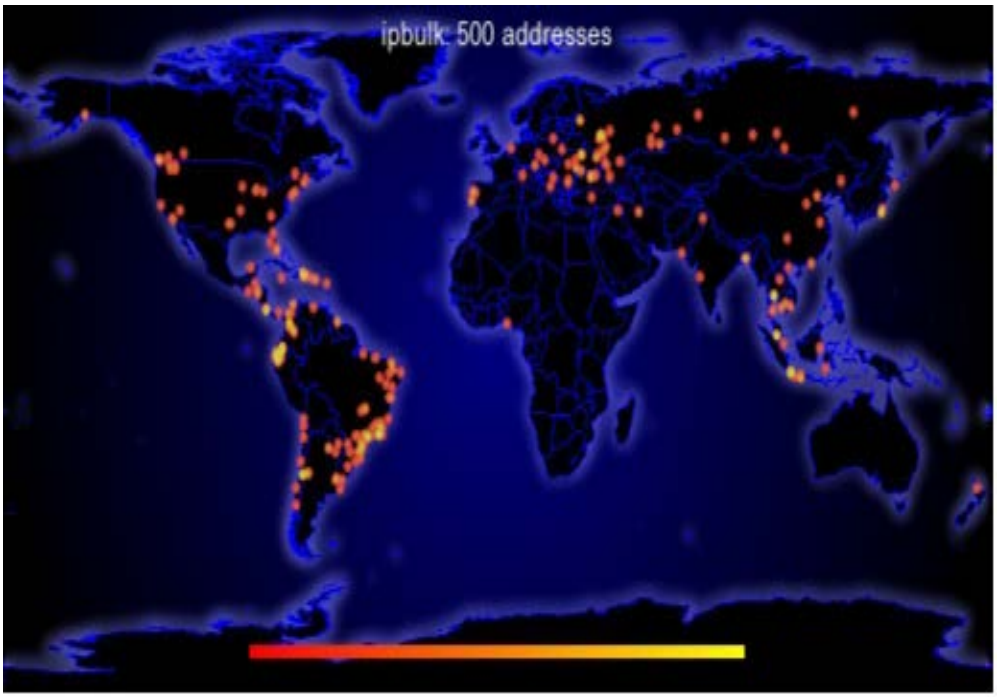
[14] Kim Zetter. "Hacker Lexicon: What are DoS and DDoS Attacks?" *Wired.* January 6, 2016. https://www.wired.com/2016/01/hacker-lexicon-what-are-dos-and-ddos-attacks/.
[15] NTIA. Communications Sector Coordinating Council. *Industry Technical White Paper*. July 17, 2017. https://www.ntia.doc.gov/files/ntia/publications/cscc_industrywhitepaper_cover_letter.pdf.
[16] Anthony Scriffignano. Dun & Bradstreet, Inc. *Briefing to the NSTAC ICR Subcommittee*. August 15, 2017.
[17] Arrabelle Hallawell. Arbor Networks, Inc. *Briefing to the NSTAC ICR Subcommittee*. August 3, 2017.
[18] Bill O'Hern. AT&T, Inc. *Briefing to the NSTAC ICR Subcommittee*. July 20, 2017.
[19] Anthony Scriffignano. Dun & Bradstreet, Inc. *Briefing to the NSTAC ICR Subcommittee*. August 15, 2017.
[20] Ann Cox. DHS. *Briefing to the NSTAC ICR Subcommittee*. August 1, 2017.
[21] Anthony Scriffignano. Dun & Bradstreet, Inc. *Briefing to the NSTAC ICR Subcommittee*. August 15, 2017.

2.3 Botnets and Automated Distributed Attacks Are Global, Making Response Complex

Infected devices, targets, bad actors, and victims are globally distributed. Bad actors include nation states, organized criminal groups, hacktivists, and individuals. The rule of law has little impact, and the offenders' ability to cover their tracks complicates attribution. Malicious actors are typically motivated by financial gain or the ability to cause a disruption of services.[22] Targets exist in the healthcare industry, academia, and the public sector; victims in the United States are more likely to pay a ransom.[23]

Over 80 percent of botnet traffic originates overseas and most traffic is designed to look legitimate. China has the most botnets, with close to 1.4 million. India is second with under a million, and Russia is third with under 600,000.[24] In the first quarter of 2017, China and South Korea "continued to top the attacking country list…Most of the attacks (50.8 percent) originated in China, followed by South Korea (10.8 percent)" with the United States at 7.2 percent."[25] Most open DNS resolvers used in attacks are outside the United States.[26]

Figure 4. Location of DNS Resolvers



Source: Bill O'Hern. AT&T. Briefing to the NSTAC Internet and Communications Resilience (ICR) Subcommittee. July 20, 2017

[22] Ibid.
[23] Raj Samani. McAfee, UK. *Briefing to the NSTAC ICR Subcommittee*. August 15, 2017.
[24] Spamhaus Project. *The World's Worst Botnet Countries*. August 18, 2017. https://www.spamhaus.org/statistics/botnet-cc/.
[25] Incapsula. *Global DDoS Threat Landscape*. 2017. https://www.incapsula.com/ddos-report/ddos-report-q1-2017.html.
[26] Bill O'Hern. AT&T, Inc. *Briefing to the NSTAC ICR Subcommittee*. July 20, 2017.

In October 2016, the Mirai botnet launched a DDoS against DNS provider Dyn. The attack disrupted some of the world's largest websites. Mirai exploits weak security on many IoT devices, continuously scanning for IoT devices accessible over the Internet that are only protected by factory default settings and contain hardcoded user names and passwords. Mirai infects devices with malware and forces them to report to a central control server, turning them into bots that can be used in DDoS attacks.[27] A relatively small number of manufacturers and their downstream vendors are known for developing vulnerable IoT devices.

Industry works internally and with law enforcement to shut down botnet hosts, but collaboration is challenging when it occurs across political borders. The U.S. Government has authorities and tools that might permit the government to take affirmative action (both offensive and defensive) against botnets, but use of such tools raises policy issues. There are complex questions around "active defense" and offensive cyber operations, including what should be conducted, how to improve the predictability of effects (as one of the key reasons for restraint is lack of predictability/precision of impacts), and who should be involved. These issues require a joint discussion and planning among the U.S. Government, foreign partners, and industry. "Active defense" means different things in different settings, and further discussion is needed.

3.0 EACH PART OF THE ECOSYSTEM MUST ADDRESS SECURITY

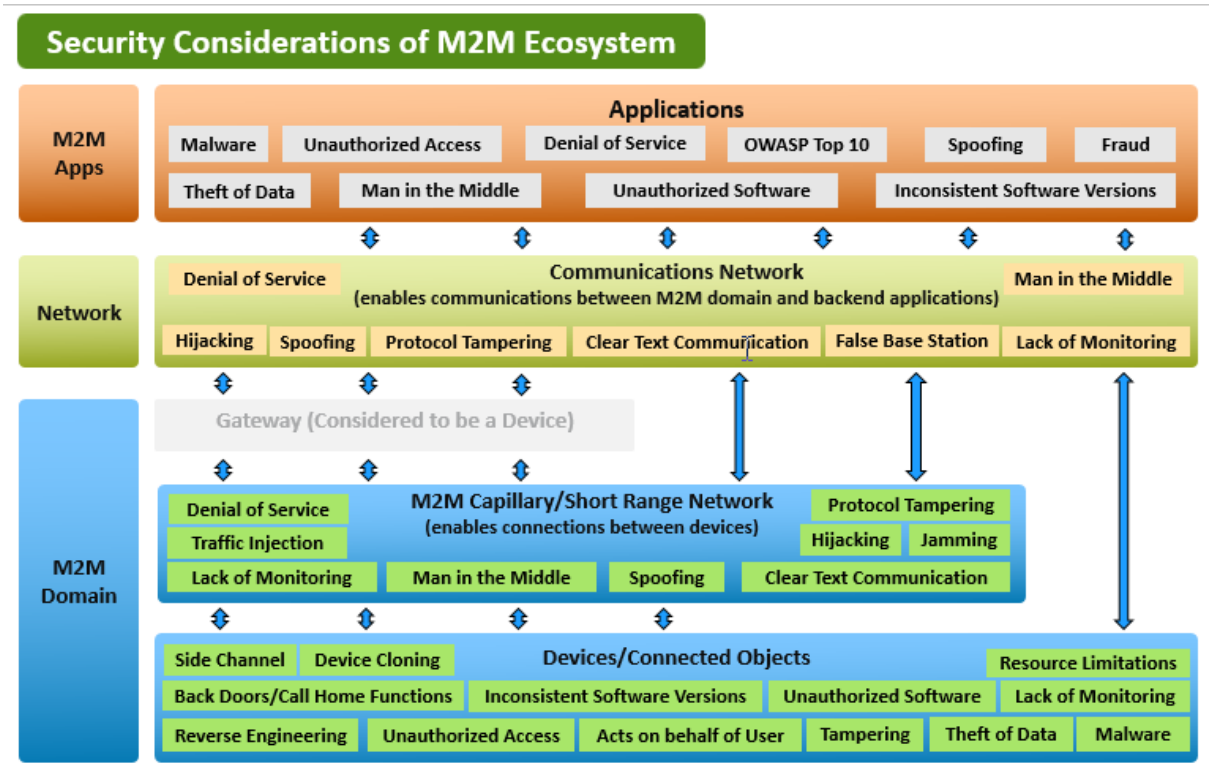
For the purposes of this report, the NSTAC divided the ecosystem into layers:

- Network (3.1)
- Consumers/Edge/Device (3.2)
- Enterprise (3.3)
- Applications/Software/OS (3.4)
- Government (3.5)
- International (3.6)

Cybersecurity demands aggressive action in each part of the ecosystem.

[27] Symantec. *Mirai: What You Need to Know About the Botnet Behind Recent Major DDoS Attacks.* October 27, 2016. https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks.

Figure 5. Security Considerations of the M2M Ecosystem



Source: AT&T Presentation on NSTAC Report to the President on the Internet of Things. November 19, 2014.

CORE FINDINGS RELEVANT TO EACH LAYER OF THE ECOSYSTEM

Several steps will help secure the Internet ecosystem from distributed and automated attacks. Different actors must contribute – individually and collectively – to create better security. This Report focuses on key actors and their roles in strengthening Internet security.

Network Layer. Network service providers have a variety of common practices in place to mitigate distributed attacks. These practices include the Network Service Providers' DDoS Common Practices; the Anti-Botnet Code of Conduct (ABC) for ISPs, and Internet Engineering Technical Forum (IETF) BCP, and the Federal Communications Commission's (FCC) Communications Security, Reliability and Interoperability Council (CSRIC) methods. The Communications Sector developed practices in the FCC's CSRIC[28] on many issues, including DDoS best practices, botnet mitigation, and implementation of the NIST *Framework for Improving Critical Infrastructure Cybersecurity*. Many providers have implemented these practices, however, other domestic and international ISPs, and those that operate networking

[28] The CSRIC and its predecessor organization, the Network Reliability and Interoperability Council (NRIC) first addressed cybersecurity best practices in NRIC VI from 2002-2004. See https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-4.

capabilities[29] also must adopt them to reduce the impact of distributed attacks.[30] Recommendations in the CSRIC report include blocking traffic destined to and from certain Internet ports, enhancing network intelligence and visibility into traffic flows, cross-ISP traffic filtering in transit in the event of a large-scale attack, and applying machine learning in the detection of botnets.

Network service providers can also help secure IoT devices that are connected to their networks; for example; wireless carriers can offer services to help manage security for IoT devices connected to Long Term Evolution or Fifth Generation (5G) networks in partnership with a variety of other players in the ecosystem. For example, AT&T, IBM, Nokia, Palo Alto Networks, Symantec, and Trustonic recently formed an IoT Cybersecurity Alliance, which is intended to drive collaboration from the member companies to develop multi-layered solutions to IoT cybersecurity challenges. Network providers are currently developing capabilities at the network layer leveraging big data analytics and machine learning to detect and mitigate IoT based attacks and are likely to continue to introduce new capabilities and services to help better manage IoT devices.

Device/Edge Layer. Device security must improve as the weaponization of devices and their potential use in DDoS attacks continues to be a major issue. While many private activities are underway, the government should convene stakeholders to drive the adoption of standards and best practices. The private sector should lead the development of standards, and the government can convene experts to demonstrate how such standards can be applied through use cases. As best practices emerge, the ecosystem may consider voluntary, industry driven device certifications that also include manufacturer support for the product lifecycle. The NSTAC previously recommended that "consideration should be given to establishing an Underwriters Lab (UL) for certification of specific securities policies."[31] The NSTAC supports the conclusion that some form of industry driven certification for IoT devices, based upon international standards, would be helpful.

To an extent, this effort is already underway. UL is developing a device certification program and other organizations such as the Cybersecurity Independent Testing Laboratory[32] (CITL) are testing devices. Consumer Reports has begun to collaborate with entities, including CITL, to consider security in device reviews, which may raise consumer awareness. In addition, the government has initiated processes, such as NTIA's work on IoT device upgradeability and NIST's Cyber Physical Systems efforts. Government and industry can drive adoption by requiring devices to meet criteria for deployment in proprietary settings. A framework for

[29] While common practices like BCP 38/84 are widely discussed in relation to ISPs, anti-spoofing technology is necessary to be deployed by anyone operating their own IP address space including enterprise businesses and other entities that provide some of their own networking functionality.

[30] See Matt Tooley, NCTA – The Internet & Television Association, Communications Sector Coordinating Council, *Industry Technical White Paper on Botnets and Automated Threats*.

[31] NSTAC. *NSTAC Report to the President on the Internet of Things*. November 9, 2014. https://www.dhs.gov/sites/default/files/publications/2012-05-15-NSTAC-Cloud-Computing.pdf, Appendix E, E-5. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

[32] Cyber Independent Testing Lab (CITL). http://cyber-itl.org/.

device deployment, developed through public-private collaboration, should recommend processes for risk management and confirm that needs differ based on functionality and context. The government should look to NIST's successful *Framework for Improving Cybersecurity for Critical Infrastructure*[33] as a model. New services are continuously being introduced to help manage and secure IoT devices. ISPs, wireless service providers, router manufacturers, security solutions providers, and others are developing services to manage IoT device security. As previously noted, wireless carriers are also collaborating with a variety of entities to bring solutions to market to help manage IoT security. Anti-virus and security firms such as McAfee and Symantec are also offering secure home services.[34] Cisco is promoting standards at the IETF, such as the Manufacturer Usage Description (MUD) standard that allows devices to self-identify in the home and may enable routers and networks to apply a security policy against the device. These are still emerging capabilities and could provide a complement to security standards in devices.

Enterprise. Enterprises must plan and manage connected devices during acquisition, use, and end of life. These organizations have many users who can be vulnerable to unsophisticated exploits but can also greatly benefit from education about security. Enterprises should also adopt best practices to ensure the redundancy and resiliency of networks, data (such as backups to protect against ransomware), cloud service offerings, and DNS. Enterprises play a key role in managing their environment by adopting and requiring security measures from their suppliers, and this approach can drive better IoT security standards across the Internet ecosystem.

Applications/Software/OS (see *Section 3.4*). The ecosystem requires increased use of secure software development and management practices. As NIST explains, "[t]here are many approaches, at varying levels of maturity, which show great promise for reducing the number of vulnerabilities in software."[35] However, use of secure software development and management practices is uneven, especially among smaller or non-traditional technology vendors with fewer resources and less expertise. Industry and government must promote best practices, support developers in start-ups, and highlight effective communication between software engineers and security experts.

3.1 Networks

FINDINGS

Networks play an integral role in defending against botnets and DDoS attacks. Network providers take a variety of actions, but more can be done to address botnets and DDoS attacks. A major challenge is encouraging adoption of existing best practices. The NSTAC identified the following techniques employed and challenges faced by industry, and developed recommendations to address these issues.

[33] National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity*. February 12, 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[34] For example, see McAfee's Secure Home Platform https://securehomeplatform.mcafee.com

[35] NIST ITL Publication. January 2017. http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=922589.

Current Activities

Network operators mitigate thousands of threats, botnets, and DDoS attacks daily, using evolving tools and enormous resources to provide their customers and other end users secure connectivity. For example, providers implement standards for anti-spoofing, block attack vectors, and detect and mitigate attacks that target or impact network service. Service providers help identify source IP addresses, filter/block emails that match signatures from blacklists, and filter/block traffic destined for phishing sites. Some of the network security techniques employed by ISPs are:

- **Best Common Practice (BCP)38.** Major carriers implement BCP38 in at least some portion of their networks. BCP38 is an IETF practice invented to prevent IP address spoofing and prevents end users from initiating traffic with a spoofed source address. Implementing BCP38 increases the likelihood that botnet traffic is either blocked because it originated with a forged source address, or is traceable so the carrier can address a security breach once identified. Most large ISPs incorporate BCP38, and an increasing number of smaller ISPs are beginning to adopt it as well.

- **Port Blocking/Filtering/Rate Limiting.** Many carriers implement port blocking, filtering, and rate limiting. These techniques are widely used in managed security services for enterprise businesses and government customers. Service providers also block certain ports on their backbones that are known to contribute to security risks. While some port blocking is done today, there is a different risk calculus in blocking or sinkholing traffic on an enterprise's network as opposed to doing so on the public Internet. ISPs are concerned about false positives in respect to Internet-wide blocking, and more aggressive blocking or filtering models may not scale. The NSTAC recognizes that there may be an opportunity to enhance these efforts, but it would require a partnership with the government to develop a policy framework supporting ISPs taking more aggressive actions to block and filter content. ISPs are necessarily conservative about these issues given the potential for false positives and the uncertain regulatory environment, especially given the FCC's Network Neutrality regulations. Moreover, many command and control sites leverage legitimate means of communication which may result in collateral damage. ISPs already block ports that are widely used in security events. AT&T, for example, attempts to isolate the threat and minimize harm to the network by blocking certain ports that transfer malicious or disruptive traffic such as Ports 25, 135, 139, 445, and 1900.[36] Other providers take similar steps. Providers also rate limit traffic for certain protocols that have nominal or limited use, or that normally consume small amounts of bandwidth (e.g., CharGen or NTP), which enables normal use of such protocols, but helps mitigate their use in DDoS attacks. Any effort to expand these activities beyond the examples above that are clearly being leveraged in cyber attacks would require collaboration with government to ensure that a policy framework was established to support these activities.

[36] See AT&T. *Network Practices*. April 24, 2017. https://www.att.com/gen/public-affairs?pid=20879; Xfinity. *Comcast List of Blocked Ports*. 2017. https://www.xfinity.com/support/internet/list-of-blocked-ports/. *CenturyLink* http://www.centurylink.com/aboutus/legal/internet-service-disclosure/full-version.html

- **NIST Cybersecurity Framework**. Industry is encouraging use of the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, implementing the framework in each core functional area identified by NIST:

  - *Identify*: identification of critical assets, information sharing.

  - *Detect*: packet sampling, signature analysis, heuristic/behavior analysis.

  - *Protect*: access control lists, policing, black/sink holes, DDoS "scrubbers," Border Gateway Protocol (BGP) flow specification, content delivery networks, anycast, end-user anti-virus software, managed security services for customers.

  - *Respond and Recover*: mitigate attack traffic, work with upstream providers to filter, and notify customers. ISPs block ports that are leveraged in ongoing attacks (for example, port 445).

- **ABCs for ISPs.** Industry encourages adoption of the U.S. Anti-Bot Code of Conduct for Internet Service Providers developed by CSRIC III, Working Group 7. The ABC is a set of voluntary practices that "address the threat of bots and botnets in residential broadband networks through voluntary participation." It emphasizes ten key principles: voluntary participation; technology neutral; approach neutral; respect for privacy; legal compliance; shared responsibility; sustainability; information sharing; effectiveness; and effective communication with consumers. Compliance with ABC requires end-user education, botnet detection, end-user notification of potential botnet infection, botnet remediation, and ISP collaboration. Potential barriers to implementation include: technology limits (current solutions may be insufficient to take down botnet threats and/or come with unintended consequences); consumer and market barriers (solutions may be viewed by customers as ineffective or undesirable—like increased consumer costs); operational barriers (impacts organization's primary mission and resources); financial barriers (difficulty in quantifying costs/benefits associated with specific recommendations); and legal, regulatory, or policy barriers (laws or policies that discourage collaboration and information sharing).

- **Traffic Management**. ISPs and network operators invest heavily in capabilities to manage traffic. Some examples include port blocking, machine learning and AI to help detect bots, destination black hole filtering and sinkholing of malicious IP addresses.

- **Consumer Notification**. ISPs commit considerable time and resources to implement consumer notifications about infections, which is a key component of the ABC principles. Based on aggregate data voluntarily and confidentially provided to the Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG), reporting ISPs notified between 98.41 percent and 99.13 percent of bot-infected customers in 2012 and between 94and 99.82 percent of bot-infected customers in 2013. But, as described below, there are limits on the utility of consumer education, and the impact these efforts have on reducing the proliferation of malware and botnets is uncertain.

- **Industry Collaboration**. The industry engages in collaboration and sharing of best practices. For example, industry – led by the IETF – is exploring collaborative solutions

such as DDoS Open Threat Signaling. Participants collaborate to identify attacks on their servers, and share information to develop threat responses before an attack occurs against other networks. The real-time exchange of telemetry between DDoS mitigation platforms facilitates DDoS mitigation and network-to-network status updates. The recent FCC CSRIC V Working Group report on information sharing provides a detailed overview of information sharing within the communications sector. Other efforts are underway including a pilot between major carriers to cooperate and disrupt the flow of traffic during a large-scale DDoS attack at their primary peering points.

- **Information Sharing.** The industry engages in information sharing as outlined in a recent FCC CSRIC V Working Group 5 report.[37] Industry shares information with trusted peers and commercial partners; government agencies under contract; law enforcement; industry peers as part of the sector policy and planning process; and, government agencies such as the DHS National Coordinating Center and the National Cybersecurity and Communications Integration Center (NCCIC).[38] DHS is also managing the International Watch and Warning Network in partnership with the Department of State to share information internationally.

- **Software Defined Networks/Network Slicing/Virtualization.** Architectural developments, such as 5G, the transition to all-IP networks, and the emergence of Software Defined Networks (SDN) and virtualization will promote security. SDN is an emerging architecture that decouples the network control and forwarding functions, enabling network control to become directly programmable. The architecture, combined with open, easily-programmable interfaces, makes it easier to mix and match solutions from different vendors and develop new capabilities. While any new approach has the potential to be compromised, SDN will help operators respond to threats due to the operator's central view of the network. Network slicing will allow 5G network operators to provide networks on an as-a-service basis. With network slicing, a single physical layer can be partitioned into multiple virtual networks, allowing operators to support different services for different customers. Services include filtering, routing, protocol limitations, and rate limiting. Operators can customize security for network slices to dynamically respond. Network virtualization includes built-in security, like isolation and multitenancy, segmentation, distribution firewalling, and service insertion and chaining.[39]

- **Managed Security Services/Consumer Security.** Many ISPs offer managed security services, such as DDoS defense services, to enterprise customers consumers to help them manage security risks. On the consumer side, ISPs offer notifications of potential infections, free anti-virus service provided in conjunction with residential broadband service, technical support to aid in remediation, among other capabilities. At the enterprise level, ISPs offer security and network monitoring and management services to the private and public sectors.

[37] FCC CSRIC V, Working Group 5 Final Report, *Information Sharing*, March 15, 2017. https://www.fcc.gov/files/csric5-wg5-finalreport031517pdf.

[38] Ibid, page 6.

[39] Bill O'Hern. AT&T, Inc. *Briefing to the NSTAC ICR Subcommittee*. July 20, 2017.

Challenges

There are several challenges with these existing solutions:

- **Legal Framework for Network Management.** Many techniques for the public Internet or consumer space involve solutions such as blocking, black holing or sinkholing IP addresses, blocking ports leveraged for malicious traffic, notifying end user customers of potential infections, and deploying IP address anti-spoofing common practices such as BCP 38/84. A challenge with these approaches is the potential for false positives and unintended consequences. Effectively remediating these issues would require ISPs to take more aggressive actions in monitoring and inspecting traffic, which raise policy concerns. For example, while there was a security exception in the FCC's prior Net Neutrality rules, the general expectation that ISPs will not interfere in traffic flow heightens risks related to some activities.

- **Encryption**. ISPs are losing visibility as more traffic is encrypted. Today, most traffic over the Internet is encrypted. And it is a simple matter for botnet operators to encrypt botnet traffic. One expert predicted that by the end of 2016, over two-thirds of the Internet's traffic would be encrypted.[40] While ISPs may have some visibility into netflow data, such as source and destination IP address, ISPs are unlikely to have broad payload visibility that may be required for aggressive blocking.

- **Internet Protocol Version 6 (IPv6).** Operators running IPv6-enabled networks require tools for security, detection, and monitoring. Due to the unique security challenges that IPv6 introduces, the ecosystem must mature security support for IPv6, improve asset discovery and detection tools to identify rogue IPv6 devices, and ensure network monitoring supports both IP Version 4 and IPv6 network assets.

- **Scalability.** Questions persist about whether solutions will work on a large scale. In enterprise, ISPs monitor IP address ranges corresponding to their enterprise customers to identify, detect, and thwart cyber attacks. It is unclear whether more granular solutions for the overall Internet will scale as large networks carry vast amounts of traffic on a given day.[41]

- **Small/Medium Sized Carriers**. A distinction must be made between large and small organizations and their capabilities in implementing BCP38 or other security measures. Small companies may require universal service funding for effective security. Companies that sell low margin Internet service and lack revenue models to cover security investments face significant challenges. The NSTAC recommends that the government should revisit the issue of incentives for deployment, particularly for small and mid-sized carriers where even a marginal investment may require incentives for such entities.

- **Consumer Notifications**. Many ISPs have notification programs but the overall effectiveness of these programs is unknown. Even when consumers receive notification of a

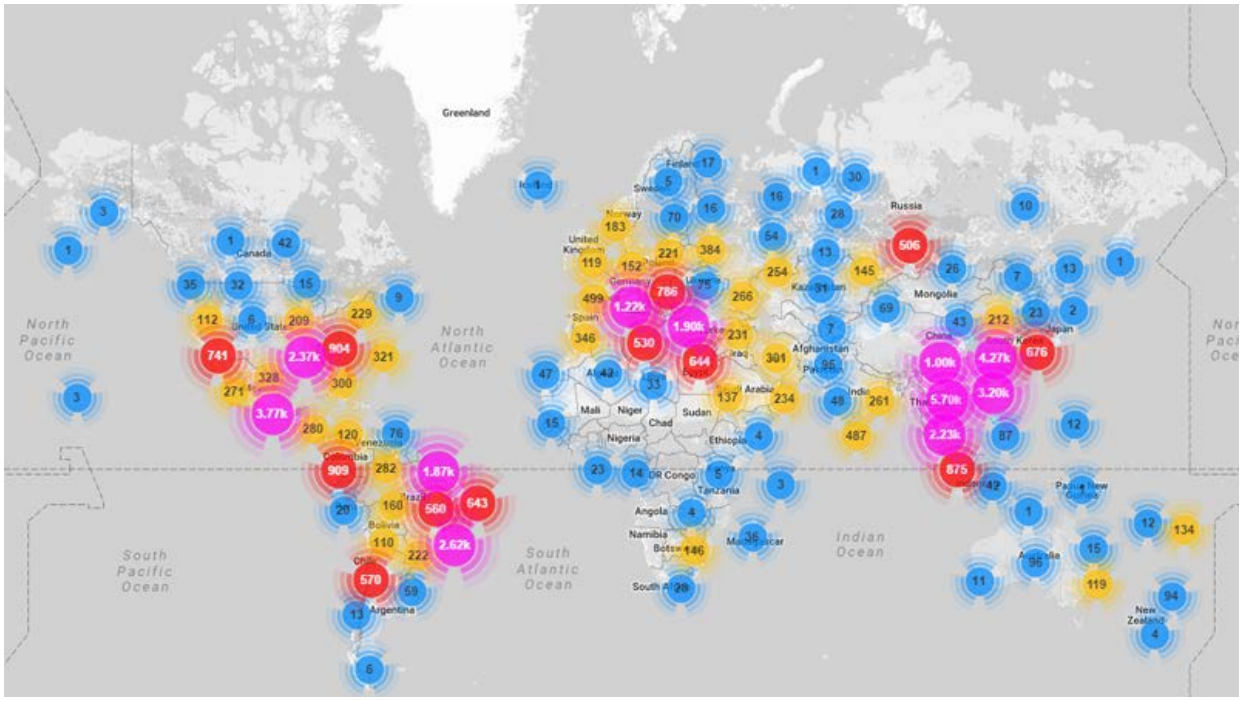
[40] Sandvine. *Global Internet Phenomena: Encrypted Internet Traffic*. 2016. https://www.sandvine.com/resources/global-internet-phenomena/spotlight/internet-traffic-encryption.html.

[41] Bill O'Hern. AT&T, Inc. *Briefing to the NSTAC ICR Subcommittee*. July 20, 2017. For example, over 168 petabytes travel over AT&T's network daily.

security issue, many lack the skills to clean their systems. There is also a high rate of reinfection, because consumers often repeat the behavior that corrupted their device in the first place.

- **International**. Botnet attacks against the United States largely originate from overseas. For example, the following map shows traffic sources for a Mirai botnet attack on August 17, 2016, which were predominantly outside the United States.

Figure 6. Traffic Sources for a Mirai Botnet Attack August 17, 2016



Source: Brian Rexroad. AT&T. Briefing to the NSTAC ICR Subcommittee. July 20, 2017.

Other Issues

The NSTAC addressed other issues regarding ISP security including the deployment of DNS Security Extensions (DNSSEC) and Secure Inter-Domain Routing. DNSSEC may not be a viable solution, as it was useful initially but as the network evolved DNSSEC was not implemented optimally, lessening its effectiveness. ISPs encounter amplification attacks, noting that several security frameworks rely on key infrastructure and validation. Network admission control and access protection help enforce validation prior to accessing the network. The major issue is trust and reputation, as each packet on the network comes with a degree of risk.

The NSTAC also reviewed Signaling System 7 (SS7) issues.[42] Although SS7 received considerable attention, SS7 itself is not the issue. Rather, interconnection and inappropriate access are the issue. (See CSRIC V, WG10 (March 2017) and May 3, 2017 Report on SS7/2FA). Industry continues to battle rogue operators who are complicit in criminal behavior,

[42] Travis Russell. Oracle. *Briefing to the NSTAC ICR Subcommittee*. August 11, 2017.

selling network identifiers and authentication to bad actors. Industry is working to enhance the vetting of interconnect (or roaming) partners and improve network hygiene.

Another issue is securing BGP routing. This includes concerns about entities publishing false routes on the Internet that can be exploited to route traffic to enable entities to monitor the traffic or otherwise conduct surveillance. The solution to this problem to date has been focused on the development of Resource Public Key Infrastructure (RPKI) that would enable ISPs and other entities to validate routes. The NIST National Cybersecurity Center of Excellence (NCCoE) has recently launched a pilot of Secure Inter-Domain Routing to explore several issues around the development of RPKI and many ISPs are participating.

RECOMMENDATIONS FOR NETWORK SERVICE PROVIDERS

- **Share actionable threat information.** ISP collaboration should include sharing of detection, notification, and planned or utilized mitigation methods within the network.
- **Increase traffic analysis.** Many ISPs perform analysis, however it should be incorporated into more robust managed security services to help enterprises manage potential DDoS attacks.
- **Adapt and apply machine learning for anomaly detection.**
- **Ensure network operators can filter malicious traffic.**
- **Encourage development of practices that result in DDoS traffic mitigation as close to the source as possible to avoid it transiting networks.**
- **Enhance the use of BCP38/84 beyond ISPs to include enterprises.**
- **Continue implementation of port blocking, rate limiting, and filtering where appropriate.**
- **Continue participation in industry efforts to increase the security of BGP.**

3.2 Consumers/Edge/Devices

FINDINGS

Weaknesses at the edge of networks, in devices that connect to networks, and from users that purchase and use devices drive insecurity. The NSTAC considered both consumers and edge devices in its research.

Consumers play a critical role. Human error can undermine industry investment in technical and software solutions. Many attacks still effectively deploy low-tech methods, such as phishing, and bad actors exploit poor cyber hygiene to launch botnet attacks. 70 percent of hacks utilize lost, stolen, or weak credentials; 60 percent of all malware uses privilege escalation or

stolen credentials.[43] The FCC CSRIC recommendations emphasized the importance of educating end-users on protective measures, such as strong passwords, anti-virus software, firewalls, and accepting updates.[44] The government has resources in place to educate consumers, however, the messages may be lost in the sheer number of tip pages, Federal Bureau of Investigation (FBI) advisories, and other communications that exist.

Users may ignore security when making purchasing decisions and may not install or configure devices appropriately. End users may not change passwords or use available security tools and may ignore available updates. Additionally, users may not wipe personal data or settings from devices when they are being replaced. Users may not have enough information, but they may also ignore available information. A survey by the Pew Research Center found 28 percent of U.S. smartphone owners did not secure access to their device with a simple four-digit personal identification number or other security feature.[45] Although the majority of smartphone users report they update their device apps or operating system, approximately 40 percent said they delayed updates until it was convenient.[46] The study found that 14 percent of smartphone users have never updated their smartphone operating system and 10 percent have never updated their apps.[47] Poor hygiene is not unique to commercial users – government users must also improve cyber hygiene. Agencies may be limited by resource constraints, and the government needs to account for costs of its future security needs. EO 13800 appropriately highlights accountability and responsibility for agency heads.[48]

Devices are critical. Many devices are developed with few security capabilities, as some vendors do not pay adequate attention to security issues. The Mirai botnet attack exploited over one million cameras with weak passwords and credentials.[49] Devices may have unchangeable default passwords, which makes them easily exploitable, or may be incapable of supporting updates, which makes it more difficult to conduct patch management in the event of a security vulnerability. The Federal Trade Commission (FTC) noted that device security will vary, but some consensus is emerging about sensible characteristics.[50] With expectations of 28 billion

[43] Ann Cox. DHS. *Briefing to the NSTAC ICR Subcommittee*. August 2, 2017.

[44] FCC. CSRIC II, Working Group 2A: Final Report. *Cyber Security Best Practices.* at 91. March 2011. https://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf.

[45] Kenneth Olmstead and Aaron Smith. "Americans and Cybersecurity." *Pew Research Center Report*. at 19. January 26, 2017. http://assets.pewresearch.org/wpcontent/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf.

[46] Ibid. at 20.

[47] Ibid.

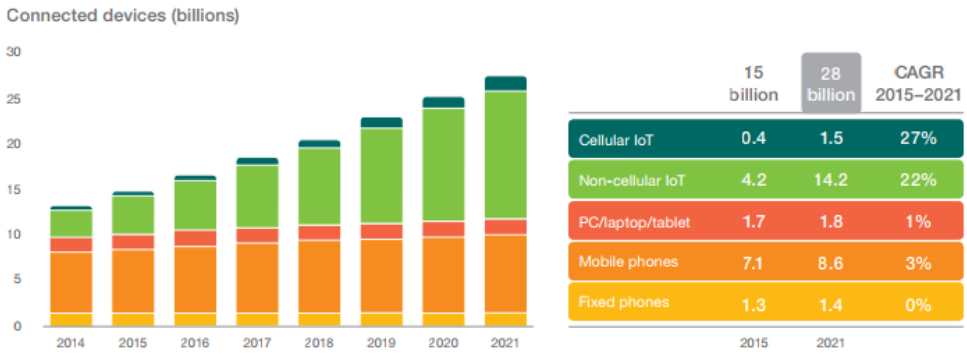
[48] White House Office of the Press Secretary. *Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. May 16, 2017. https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

[49] Lorenzo Franceschi-Bicchierai, *How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet.* September 29, 2016. https://motherboard.vice.com/en_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs.

[50] Thomas B. Pahl. FTC. *Start with security – and stick with it*. July 28, 2017. https://www.ftc.gov/news-events/blogs/business-blog/2017/07/start-security-stick-it ("When it comes to data security, what's reasonable will depend on the size and nature of your business and the kind of data you deal with."); Internet of Things: Privacy & Security in a Connected World. FTC. n.130. January 2015. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf ("There may be other appropriate measures, as the security measures that a

connections by 2021, and 73 percent of global Internet traffic being mobile,[51] networks or people alone will not be able to provide security for all these devices.

Figure 7. Growth in Connected Devices



Source: Ericsson Mobility Report (June 2016)[52]

The weaponization of IoT devices presents a significant challenge. Poorly-secured, always-on devices compromised by botnets could have catastrophic consequences. IoT providers and their end-users are sometimes apathetic to the harm that vulnerable devices can cause, and may have little incentive to invest in security beyond that required to ensure operation of the device.

IoT should support updates and a system for authentication and validation.[53] Novel malicious protocols can defeat outdated security models, so older security needs to be upgraded. Network service providers may be able to help manage non-secure devices in the network but there are complicating factors. For example, approximately 70 percent of Internet traffic globally is encrypted, and that figure is expected to grow.[54] Adding to the complexity, many consumer devices are not publicly addressable and operate behind home routers and network address translation systems that are not managed by the ISPs. Users often have multiple routers. Some companies, including ISPs and security solutions providers are experimenting with security management services, but the market potential is uncertain.

Security is not limited to the device layer. We cannot rely entirely upon building security into devices to address security. For example, network providers can perform analytics on traffic traversing their networks and apply machine learning to help identify and mitigate threats to

company should implement vary, depending on the risks presented by unauthorized access to the device, and the sensitivity of any information collected.").

[51] Ericsson Mobility Report. *On the Pulse of the Networked Society*. June 2016. https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf; Cisco. *Cisco Visual Network Index: Forecast and Methodology, 2016-2021*. White Paper. June 7, 2017. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html.

[52] Ericsson Mobility Report. *On the Pulse of the Networked Society*. June 2016. https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf.

[53] Raj Samani. McAfee, UK. *Briefing to the NSTAC ICR Subcommittee*. August 15, 2017.

[54] See Sandvine. *Global Internet Phenomena: Encrypted Internet Traffic*. 2016. https://www.sandvine.com/resources/global-internet-phenomena/spotlight/internet-traffic-encryption.html.

some IoT devices. There have also been proposals like the Cisco MUD standard which is being introduced at the IETF. MUD would allow devices to self-identify and be placed by routers and other networking equipment into distinct classes of service applying rate limits and white lists to manage security. In addition, companies such as McAfee are starting to offer home device security management services. These efforts are in their infancy but can improve security as the market evolves.

Supply chain is also important. Carriers are improving defenses, but they cannot do it alone. Chipmakers and platform vendors must increase efforts and the ecosystem must promote emerging "bolt on" security upgrades to home networks. Industry and the government must focus on security marketing, acknowledge shared responsibilities, and encourage teamwork.

The NSTAC acknowledges that there are varying opinions on the role of government in IoT security. It is clear, however, that there must be a focus on mitigating these vulnerabilities.

Current Activities

Numerous innovations are being developed to address the end user and device layer. Chipmakers and platform vendors are building additional security into unsophisticated IoT devices.[55] As the Consumer Technology Association (CTA) explained:

- Intel Collaborative Research Institute for Secure Computing has developed a TrustLite security framework to enhance security for small IoT devices.[56]
- Altera Field Programmable Gate Arrays or Systems on a Chip use hardware crypto acceleration and AES-secured remote software upgrades.
- Analog Devices' IoT products use crypto hardware acceleration, secure boot, and in-circuit memory read protection.
- Apple, Qualcomm, Samsung Electronics, and others use chips with ARMS's TrustZone.
- IBM, Microsoft, Intel, NXP, Panasonic, and Samsung's IoT platforms have built-in security or security guidance for implementers.

Consumer Network Monitor Devices (NMDs) and smart routers are becoming more prevalent. Consumer NMDs contain specifications that include Virtual Private Network (VPN) mode, DoS attack protection, unauthorized access blocking, and virus and malware scanning. Smart routers now come with similar features. The industry is designing hardware capable of providing "bolt on" security upgrades to consumers' home networks.

Industry provides several tools to customers to help protect devices. These include providing antivirus tools to consumers to help detect viruses and clean up machines; threat analysis from a

[55] Mike Bergman. Consumer Technology Association. *Briefing to the NSTAC ICR Subcommittee*. August 3, 2017.
[56] Koeberl, Patrick, et, al. "TrustLite: A Security Architecture for Tiny Embedded Devices." http://www.icri-sc.org/fileadmin/user_upload/Group_TRUST/PubsPDF/trustlite.pdf

network perspective; notifying end users and providing self-remediation tools and paid care options; and providing DDoS mitigation service for subscribing customers.

There are voluntary guidelines and best practices to mitigate device vulnerabilities and increase consumer awareness, and industry is also building upon these efforts.

- Groupe Spécial Mobile Association (GSMA), for example, has developed guidance for developing secure IoT products and services, including for IoT endpoint device manufacturers.[57]

- CTA is developing robust best practices to enhance security of in-home connected devices.[58]

Industry is working with the government to provide resources for IoT security at the end user stage. For example, industry members are collaborating with NTIA in a multi-stakeholder process to develop a common lexicon for IoT upgrading. As part of that process, working groups have identified guidance on the topic from over 30 U.S. and international organizations,[59] features to secure over-the-air updates, and guidance for communicating about IoT upgradability to consumers.

RECOMMENDATIONS FOR CONSUMERS/EDGE/DEVICES

- **Establish and Promote Consensus Device Security Guidelines**. Devices should be hardened with basic cyber hygiene practices, including the ability to receive upgrades and patches. Several government efforts look to increase cybersecurity hygiene, but more is needed.[60] Government and industry should determine whether minimum-security expectations need to be developed. Device manufacturers, particularly IoT device development kit manufacturers, need to assure good tools are included and use secure default configuration, automated patching, and the ability to recover from malware infections.[61]

- **Promote Home Management Services**. The government should support industry investment in home management services, which would oversee operations of connected devices within the home. This capability could be offered in routers or as a separate device within the home.

- **Promote Consumer Awareness/Education**. Industry should continue to educate users, including about the importance of completing updates. The government should amplify and

[57] See GSMA IoT Security Guidelines. https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/.
[58] Consumer Technology Association. *Project Overview: Securing Connected Devices for Consumers in the Home*. CTA-CEB33. July 7, 2017. https://standards.cta.tech/apps/group_public/project/details.php?project_id=429.
[59] See NTIA. *Catalog of Existing IoT Security Standards (Draft Version 0.01), NTIA Multistakeholder Process on IoT Security Upgradability and Patching, Existing Standards, Tools, and Initiatives Working Group*. July 2017. https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog.pdf.
[60] Arabella Hallawell. Arbor Networks, Inc. *Briefing to the NSTAC ICR Subcommittee*. August 3, 2017.
[61] See draft NIST. Special Publication 800-193. *Platform Firmware Resiliency Guidelines.* May 2017. https://csrc.nist.gov/csrc/media/publications/sp/800-193/draft/documents/sp800-193-draft.pdf

coordinate its messaging. There are existing campaigns, such as STOP.THINK.CONNECT, which can be used for this purpose.

- **Support Enhanced Information Sharing**. The government should encourage information sharing among device manufacturers, including safe harbors and liability protection.

3.3 Enterprise

FINDINGS

Enterprise users and systems play a vital role. Enterprises – companies with hundreds of thousands of devices, government agencies whose constituents depend on connectivity, small businesses that deploy industrial sensors and bring your own device (BYOD) – are affected by botnets in two ways. First, enterprises are targets of botnet attacks. Second, enterprises have concentrations of IoT devices that could be leveraged as part of a global botnet if left vulnerable.

For years, adversaries have used botnet-enabled DDoS attacks to disrupt enterprise operations. Enterprises may be the target of DDoS attacks due to nation states targeting U.S. infrastructure, hacktivists trying to make a statement, criminals distracting from more insidious attacks, or other enterprises attempting to disrupt competition. As enterprises' IT, physical infrastructures, and business continuity become dependent on IP-enabled devices, enterprises become more susceptible to long-term or permanent disabling of their operations; what some are calling "destruction of service." Even if businesses are not themselves the target of botnets, their vulnerable devices can serve as a gateway for penetration of their networks, theft of high value data and even destruction of IT and operational infrastructures from within. An enterprise's own IoT devices can be used to launch a DoS attack against the enterprise itself due to the proliferation of connected devices on almost every enterprise's network.

The sheer number of devices makes it harder for organizations to track devices, increasing the risk of theft and leaving devices vulnerable to attacks. Enterprises of all sizes must manage more points of interaction on their networks, including VPNs, to facilitate off-site access. This increase in connectivity exposes enterprises to additional threats, including threats from devices whose security may not be sophisticated. The need for provisioning, monitoring, updating and end of life management may be more of a challenge than existing companies' IT departments can handle.

The botnet threat to enterprises goes beyond attacks on devices. A major challenge is protecting against attacks on shared resources that the enterprise uses to conduct business. As enterprise services span their internal IT network, cloud offerings, and shared resources, they must protect against a business-impacting incident on one of those services. For example, many businesses' Internet presence went offline when their DNS services were halted during the October 2016 Mirai attack on Dyn.

Enterprises can play a significant role in mitigating botnet threats. Enterprise IoT deployments within internal networks should be more manageable with the application of appropriate security technologies that are commensurate with identified risks. To reduce enterprise risk, these security capabilities must be delivered consistently across the IoT value chain to enable the

visibility and automation necessary for enterprises to prevent cyber threats from targeting connected elements, and protect the networks and controller environments from device-initiated attacks. These capabilities must be natively integrated, with high levels of automation across functions to rapidly identify advanced attacks and ensure that preventative security controls can be enforced across all environments in near-real time. Within the context of IoT deployments, preventing cyber threats across the entire enterprise IoT value chain requires at a minimum: (1) security of the endpoints; (2) security of local networks; (3) security within associated service provider networks; and (4) security of cloud environments and IoT host controllers.

As an example, the Marine Corps takes an aggressive approach to enterprise management.[62] The Marine Corps tracks every device that tries to connect to its network, and ensures that the device is fully patched and compliant with security protocols before connecting. The Marine Corps maintains a strict policy for personal devices. Where BYOD is permitted, devices are placed in virtual containers to protect data on the device and the government network. The Marines also ensure that users have the minimum privileges to carry out their responsibilities, utilize two-factor authentication, and audit users for every file creation, modification, and deletion. Although this approach is more aggressive than what most enterprises can do, it shows steps that could be taken as part of a program to secure enterprises from botnets and other threats.[63]

One of the NSTAC's findings is that IoT devices have a vast range of characteristics and capabilities. Within an enterprise environment, some high value IoT assets that have advanced processing capabilities, such as automobiles, may carry a degree of cybersecurity risk that makes deployment of a dedicated endpoint security solution viable. However, many other enterprise IoT devices lack individual computing power and instead rely on the command and control functions of controller hosts for security enforcement. Further, a large percentage of enterprise IoT platforms and controllers are dependent on cloud connectivity that may be hosted within internal data centers, public clouds, or in-service provider environments. Consistent, well-integrated security across all these platforms and controllers, regardless of their location, is critical to prevent compromise and the execution of unauthorized command and control activity that could leverage large swathes of enterprise IoT devices for automated and distributed attacks.

Promising innovations are poised to help enterprises: SDN and network functions virtualization (NFV), and other approaches will refine how systems are architected and organized, and will permit creative security measures. SDN will offer several advantages to enterprise security:

- Centralized control: offers an improved security vantage point;
- Management: security management improves with full network visibility;
- Applications: SDN applications provide native security control functions;
- Data Collection: native collection and analytics offer enhanced response; and

[62] Ray Letteer. U.S. Marine Corps. *Briefing to the NSTAC ICR Subcommittee*. August 29, 2017.
[63] Ibid.

- Efficiency: SDN enables more immediate re-routing and infrastructure changes (Dynamic Enforcement).[64]

NFV is also promising. The European Telecommunications Standards Institute explains[65] that NFV in 5G will support network slicing, which is the creation of multiple logical network instances (i.e., slices) on the same network, which can be leveraged to deploy and manage network slices in an automated and flexible manner. Cloud-native design principles maximize efficient use of enterprise resources through finer-grained multiplexing on the infrastructure. End-to-end service management, i.e., enabling different service offerings for different customers, permits customers to select basic network service components that best meets their needs. Edge computing, with highly distributed systems allows network functions to run on servers closest to the end-user device, i.e., on the "edge" of the network architecture. Cloudification of the Radio Access Network is expected to provide operators with unprecedented capability in terms of flexibility, agility, resource/service management and orchestration. Multi-site/domain services, including the support of Infrastructure as a Service, NFV as a Service and Network Service composition in different administrative domains is critical in the transition to 5G. NFV License Management, standardizing the underlying license management mechanisms would avoid compounding the complexity of licensing. These innovations promote security, reliability, and scalability in enterprise security.

Enterprises should establish some clear objectives to address these risks, including the following:

Mitigate the risk of traditional botnet attacks against enterprise networks. Enterprises must explore all available methods to mitigate the risk of traditional botnet attacks directed at their networks. This includes working with Internet service providers to implement network-level defenses such as port blocking, traffic flow routing, and anti-spoofing and other attribution methodologies in advance of DoS attacks. Many enterprises look to their network providers to deliver controls or functionality as part of managed security services that can restrict devices from any communication with domains outside of authorized controllers and enable advanced security solutions like application-based firewalls supported by vast amounts of dynamic threat intelligence.

Ensure that devices have built in security at the time of purchase and for their product life-cycle. Enterprises can take several steps to ensure that connected devices run securely on their networks. These steps include considering device security at the time of purchase; asking potential suppliers a variety of questions about how the suppliers secures devices, including how to authenticate to a device and how to patch or update a device; and potentially having devices tested by an independent organization. Many enterprises have significant buying power and can drive better overall security during the design and production phases of the device development lifecycle.

Post-deployment, enterprises must understand and employ all available methods to prevent devices from being conscripted (or used to attack its own networks). In securing devices on their networks, the most important considerations for enterprises are: detection (the ability to

[64] Bill O'Hern. AT&T, Inc. *Briefing to the NSTAC ICR Subcommittee*. July 20, 2017.
[65] ETSI NFV Industry Specialization Group. *Network Operators Perspectives on NFV Priorities for 5G*. February 21, 2017. https://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf

detect all connecting devices in real time), segmentation (the ability to segment or "wall off" endpoints from other parts of their networks, and automation (the ability for selected solutions to function in an automated manner), which are critical to achieve scale as the number of connecting devices increases exponentially. A variety of options exist that provide these features, including tools that allow enterprises robust authentication of devices; tools that enable behavioral profiling of devices (the ability to detect abnormal device behavior that might indicate compromise); and scanning techniques that allow enterprises to hunt for vulnerabilities and malware more actively, so as not to disrupt device operations. Enterprises should be attuned to emerging approaches and tools that will assist them in securing devices on their networks, including security information and event management and orchestration platforms that allow for real-time analysis and sharing of contextual information.

RECOMMENDATIONS FOR ENTERPRISES

Motivating and enabling enterprise security is difficult, in part because of the diversity in enterprise settings and needs. The NSTAC has identified several steps that should be taken:

- **Consider the applicable recommendations above for consumer devices as tools for improving the security posture in enterprise environments, especially for BYOD.**

- **Improve awareness of best practices.** DHS and other agencies should work with industry verticals, represented by industry groups (and, for enterprises deemed "critical infrastructure," their Sector Coordinating Councils) to ensure awareness of best practices for mitigating the effects of botnet attacks and for securing connected devices. Where possible, DHS and industry should provide industry specific practice guides. In addition, DHS should build upon the work being done at NCCoE.

- **Consider incentives to promote adoption of standards.** Federal agencies and Congress should consider utilizing federal funding to incentivize the adoption of this Report's recommendations in federally funded projects and for the businesses that implement the projects. These incentives would only be applicable in instances where requirements for securing devices that are directed or overseen by the Federal Government (such as for medical devices) are not already in place.

- **Deploy managed security services.** Enterprises of all sizes and types should consider deploying managed security services. Every organization needs to evaluate its security posture and carefully consider whether to deploy some sort of managed security approach. In addition, monitoring capabilities should address all types of connected devices. Services like DDoS mitigation in the event of attacks facilitated by botnets are useful, as companies are increasingly going to be held accountable for security.

- **Address enterprise security.** Enterprises should leverage network isolation, micro-segmentation, and filtering techniques to secure and restrict access to the Internet. Other options that can help enterprise security include:

    - *Domain awareness:* Enterprises should track and block traffic from domains that host threats. Enterprises should also take steps to protect their domains. Attackers

often target domains with the largest DNS entry to amplify the effectiveness of their attack.

- *Deploy compensating controls where appropriate.* Not every organization will be able to deploy prescribed protocols. As NIST explains, in an industrial setting, "there may be situations where the [industrial control system or ICS] cannot support security controls or control enhancements, or where the organization determines it is not advisable to implement those through ICS. In such a situation, the organization provides rationale describing how compensating controls deliver an equivalent security capability or level of protection for the ICS, and why the related baseline security controls could not be employed."[66] Examples of such controls include network-aware real-time detection, authentication and authorization, vulnerability management, behavior profiling, segmentation, and mitigation.[67] Compensating controls will not solve the global botnet problem, but they are an important step in protecting enterprises.

- *Leverage the cloud.* Established cloud service providers have increased their security posture and can offer enterprises significant security advantages. Enterprises – private and government – should explore cloud providers and the security they can offer.

- *Use dynamic provisioning.* This is an important part of network virtualization and segmentation, enabling companies to speed up and better control how devices and users are authorized to be on a system. Dynamic provisioning automates IT processes and enforces security requirements, and enables more rapid responses to security issues.

- *Redundancy.* All enterprises should look at redundancy for DNS and all business-critical Internet services.

- **Consider the insurance market.** The insurance market may drive improvement as underwriters probe companies on the maturity of their security risk management practices and offer lower premiums to companies higher on the maturity scale.

3.4 Applications/Software/OS

FINDINGS

Software in applications and operating systems plays a critical role in successfully addressing botnets, which is intensifying as software is integrated into more systems and devices. Moreover, as software has proliferated, many non-traditional technology companies have become providers. While there has been significant improvement and sharing of secure software

[66] NIST ITL Bulletin. *Tailoring Security Controls for Industrial Control Systems*. November 2015. http://csrc.nist.gov/publications/nistbul/itlbul2015_11.pdf.

[67] Wallace Sann. ForeScout. *Briefing to the NSTAC ICR Subcommittee*. August 22, 2017.

development and management processes, non-traditional software providers, start-ups, and others may not be aware of or have resources to implement the processes. Moreover, in the IoT context, risk from software vulnerabilities can be elevated; connected cars could crash, and smart toasters could cause a fire.[68]

Botnet Challenge Relevance to Applications/Software/OS

Applications, software, and operating systems are critical because they are key to endpoint security and to the security of services or resources that are leveraged by endpoints. Multiple developers provide software embedded in devices, applications and services; this diversity is integral to innovation, but presents a security challenge. Stakeholders are at different levels of maturity in software development and software management. While software development is key to limiting the number and severity of vulnerabilities in software from the outset, management is key to ensuring that vulnerabilities that are discovered can be addressed.

It is impracticable or impossible to develop software without any vulnerabilities. While progress is being made in formal methods of verification for small, highly critical pieces of vital systems, using such methods at scale or for complex cyber-physical systems is still a mid- to long-term challenge.[69] Instead, implementing secure software development and management best practices, guidelines, and tooling can raise baseline security.

However, despite the availability of vendor practices, guidelines, and tooling, awareness and implementation by both vendors and customers lags considerably. First, not all software is developed or managed by large scale vendors, and secure development practices cannot necessarily be easily or consistently applied in smaller development environments. Second, open source code is increasing; it is often maintained by volunteers who may not have requirements or processes for secure development, clear accountability, or funding to respond to security issues. Third, users can interrupt implementation, and many struggle to implement security patches or mitigations on products, services, or devices in the consumer and enterprise contexts.

Efforts Are Underway to Address the Threat

Software vendors began working to improve code security, i.e., software development, over 15 years ago. This area of practice, often referred to as software assurance, encourages developers to build more secure software and address security compliance requirements. Many large vendors have developed programs, training, and tooling for code development, implementation, and refinement. For example, use of the Security Development Lifecycle (SDL) ensures that software is designed, developed, and deployed with security in mind throughout its entire lifecycle.[70] Vendors have collaborated through non-profits like the Software Assurance Forum

[68] Charlie Mitchell. Inside Cybersecurity. *Black Hat founder sees software liability as major cybersecurity policy challenge.* July 26, 2017. https://insidecybersecurity.com/daily-news/black-hat-founder-sees-software-liability-major-cybersecurity-policy-challenge.

[69] Kevin Hartnett. WIRED. *Computer Scientists Close in on Perfect, Hack-Proof Code.* September 23, 2016. https://www.wired.com/2016/09/computer-scientists-close-perfect-hack-proof-code/.

[70] Microsoft. What is the Security Development Life Cycle? https://www.microsoft.com/en-us/sdl/default.aspx.

for Excellence in Code (SAFECode) to promulgate practices for software assurance.[71] Vendors have contributed to developing International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 27034, a process-based international standard for specifying, designing/selecting and implementing information security controls.

Software vendors have been working to improve software management by developing, implementing, and promoting coordinated vulnerability disclosure (CVD) policies, processes, and programs. Vulnerability disclosure and handling involves communicating with third party finders; validating and triaging vulnerabilities; developing an update to mitigate the vulnerability (e.g., "patch"); and applying updates or mitigations to systems that are in operation. As with tools to improve code assurance, technology providers have invested in best practices for vulnerability disclosure and handling. There are two ISO standards, ISO/IEC 29147 and ISO/IEC 30111, which describe processes for receiving vulnerability information from third party finders, communicating with finders about reported issues, and investigating, triaging, and resolving vulnerabilities.

Some technology providers have invested in promoting CVD, and the U.S. Government also has increased its effort in this area.[72] Numerous software vendors have participated in NTIA's multi-stakeholder process around vulnerability disclosure and handling to increase adoption of existing best practices, improve response to complicated disclosure challenges involving multiple parties, and help safety critical industries better understand how to adopt CVD.[73] Building from the NTIA effort, the Food and Drug Administration released guidance encouraging medical device manufacturers to adopt CVD, referencing ISO/IEC 29147 and ISO/IEC 30111,[74] and the National Highway Transportation Safety Administration released guidance encouraging auto manufacturers to have a method and policy for receiving vulnerability reports from security researchers.[75] In addition, the Department of Defense (DoD) and the General Services Administration have created CVD programs and/or bug bounty programs, enabling coordination with researchers.[76] Most recently, the Department of Justice (DOJ) issued a framework to assist organizations in creating a voluntary coordinated cyber vulnerability disclosure program. Congress is considering the issue as well. While it may not be appropriate for every organization, CVD could help address software management challenges.

---

[71] SafeCode. https://safecode.org/about-safecode/.

[72] I Am the Cavalry. *DOT Gov Coordinated Disclosure Timeline*. https://www.iamthecavalry.org/wp-content/uploads/2016/12/IATC_Gov-Coordinated-Disclosure-Timeline_v1.0.jpg.

[73] NTIA. Multi-stakeholder Process: Cybersecurity Vulnerabilities. 2016. https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

[74] Department of Health and Human Services (HHS). "Postmarket Management of Cybersecurity in Medical Devices—Guidance for Industry and Food and Drug Administration Staff." December 28, 2016. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

[75] National Highway Traffic Safety Administration (NHTSA). "Cybersecurity Best Practices for Modern Vehicles." October 2016. https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

[76] DOD. "DOD Announces Digital Vulnerability Disclosure Policy and "Hack the Army Kick-Off." *Press Release*. November 21, 2016. https://www.defense.gov/News/News-Releases/News-Release-View/Article/1009956/dod-announces-digital-vulnerability-disclosure-policy-and-hack-the-army-kick-off/; https://hackerone.com/deptofdefense; GSA. Vulnerability Disclosure Policy. https://18f.gsa.gov/vulnerability-disclosure-policy/.

RECOMMENDATIONS FOR SOFTWARE DEVELOPERS

Efforts to improve software assurance and manage and respond to reported or otherwise discovered vulnerabilities have demonstrably improved cybersecurity, but work to create a mix of incentives and disincentives could help. To that end, the NSTAC recommends the following considerations:

First, policies focused on software assurance and vulnerability management – regardless of the implementing mechanism – must leverage international standards, including IEC/ISO 27034, ISO/IEC 29147, and ISO/IEC 30111. They must focus on the processes used to develop and fix software (i.e., how software is built to reduce the number of vulnerabilities and how vulnerabilities are patched or mitigated) rather than the presence of vulnerabilities.

Second, neither governments nor businesses have effectively leveraged market forces to drive the development of more secure software because it is not yet clear what standard market forces should meet. The NSTAC recommends that the U.S. Government foster awareness of the role that software assurance and technology purchases have on operational risk. The government should also emphasize existing best practices and standards, enabling Information and Communications Technology (ICT) buyers to have conversations with their suppliers about technology product and service development and security management practices.

The NSTAC specifically recommends the following:

- **Government and educational institutions should strive to make security part of the Computer Science curriculum within the Science, Technology, Engineering, and Math initiative.**

- **The software development community should provide guidelines on DevSecOps processes.**

- **Industry should consider reasonable and prudent coordinated vulnerability disclosure programs.** These could include organization-managed CVD programs or outsourced programs if organizations don't have the capacity to manage them internally.

- **Industry should give developers the tools to code securely.** Improve code development tools to enhance traceability and security.

- **Share best practices to deal with vulnerabilities.** NTIA has reviewed this issue,[77] and industry can support recommendations that derive from that multi-stakeholder process, as well as other guidance.[78]

[77] NTIA. Multi-stakeholder Process: Cybersecurity Vulnerabilities. 2016. https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

[78] DOJ. "A Framework for a Vulnerability Disclosure Program for Online Systems." July 2017. https://www.justice.gov/criminal-ccips/page/file/983996/download.

- **The government should consider liability protection for those who publicly address vulnerabilities.** The Nation may need a paradigm shift in how it approaches these challenges.

- **The government and industry should collaborate on a campaign to promote software assurance – validating software to limit security vulnerabilities.** This may require promotion of best practices or guidelines to set an example for software developers.

- **Carefully consider how to secure open source development.** Industry's collective effort to provide funds to critical elements of the global information infrastructure through the Core Infrastructure Initiative will help to address some issues, however, the NSTAC believes that more effort is needed.

- **Government and industry should increase technology user understanding of the importance of timely patching.** This can be done by incorporating these components into existing security awareness programs.

3.5 Government

FINDINGS

The government plays a key role in Internet and communications resiliency. It is a purchaser and manager of connected devices; it is a regulator or convener in the shaping of policy; and it wields sovereign power to prosecute criminals, defend the Nation, and negotiate with other countries. Each role is different, presenting different challenges and offering different opportunities.

As a manager and purchaser, the government confronts many of the same botnet challenges as other enterprise users. The number of connected device users within the government makes device management difficult. The government has the added responsibility of securing sensitive government information, as well as citizen data – making the government a high-value target. In addition, U.S. Government entities manage several vulnerable IP blocks.[79] It faces further challenges in the regulatory and procurement policy environment, which restricts flexibility and necessitates procurement decisions be made far in advance and subject to oversight and external constraints.

The government has unique opportunities to enhance security. As a manger, the government can take steps to improve mobile use management practices – utilizing any number of existing device management services and increasing awareness of the importance of employing basic cyber hygiene practices. As a procurer of technology, the government can demand more secure devices. Government standards often lead to private sector adoption of those standards, avoiding the development of different and potentially competing practices. Senator Mark Warner introduced a bill, the *Internet of Things (IoT) Cybersecurity Improvement Act of 2017*, which proposes to improve IoT security by establishing minimum requirements for IoT devices

[79] Ann Cox. DHS. *Briefing to the NSTAC ICR Subcommittee*. August 1, 2017.

procured by the Federal Government.[80] Legislation like the *IoT Cybersecurity Act*, however, could have unintended consequences if not carefully approached. The current draft, if enacted, could expose government contractors to liability due to onerous certification requirements, encourage "hacking" of government devices, and limit contractors' ability to appropriately manage vulnerability disclosures. Cybersecurity is best ensured through flexible, market-driven solutions that reflect private sector leadership and innovation and which are developed through collaboration between industry and government.[81]

As a regulator or convener, the government can shape policy and standards, while promoting innovation. In the United States, cyber policy emphasizes the government as a convener. The government should continue to bring stakeholders together to develop best practices with stakeholders from a diverse selection of industry and across the communications and ICT ecosystem. It is imperative that the government bridge the knowledge gap between sophisticated and unsophisticated industries. Internationally, the government can facilitate collaboration on a larger scale, encouraging other countries to share information and adopt appropriate best practices to mitigate botnets. These efforts could markedly reduce the number and magnitude of such attacks, as many originate overseas.

The government plays an important part in securing funding for research on cybersecurity and attack mitigation – the benefits of which cannot be overstated. In addition to direct spending, the government should continue to look for opportunities to engage with the public to enhance security. This year, the FTC hosted a prize competition to create solutions to "guard against security vulnerabilities in software found on the IoT devices in their homes."[82] The winner – a software developer from New Hampshire – developed a mobile app that can help users determine whether their devices are out of date or their networks are insecure.[83]

The government also has a unique role in public safety and should work with NIST and others to increase security of public safety systems. Enforcement actions by the FTC against manufacturers employing woefully inadequate security measures put industry on notice of the need to implement basic security and truthfully represent the security of their devices to consumers.[84]

As a sovereign nation, the government has unique powers and duties to protect citizens, enforce the law, and defend the country from external threats, including botnets. Through these powers,

[80] Mark Warner. "Senators Introduce Bipartisan Legislation to Improve Cybersecurity of "Internet-of-Things" (IoT) Devices." *Press Release*. August 1, 2017. https://www.warner.senate.gov/public/index.cfm/pressreleases?ID=06A5E941-FBC3-4A63-B9B4-523E18DADB36.

[81] Mike Bergman. Consumer Technology Association. *Briefing to the NSTAC ICR Subcommittee*. August 3, 2017.

[82] FTC. IoT Home Inspector Challenge. 2017. https://www.ftc.gov/iot-home-inspector-challenge.

[83] FTC. "FTC Announces Winner of its Internet of Things Home Device Security Contest." *Press Release*. July 26, 2017. https://www.ftc.gov/news-events/press-releases/2017/07/ftc-announces-winner-its-internet-things-home-device-security.

[84] FTC. "FTC Approves Final Order Settling Charges Against TRENDnet. Inc." *Press Release*. February 7, 2014. https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc; https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.

the government can stop or deter some malicious activity. Examples of effective tools include domain registration blocking, IP blocking, and criminal investigations and botnet takedowns.

Private-public-partnerships with law enforcement have been effective, and the U.S. should look for opportunities to expand these efforts. Law enforcement, computer emergency response teams, and others often rely on the private sector for threat intelligence and data from telecommunications providers, anti-virus vendors, and the financial sector. Intelligence is essential to identifying individuals with the motivation, intent, and backing to conduct cyber attacks, and these partnerships help governments and ISPs globally to identify and remediate threats. The NSTAC recommends that the government increase collaboration with the private sector, particularly with respect to investigations. Such public-private partnerships have flourished in the United Kingdom, and U.S. security companies and others stand willing to cooperate with government to support pending and future investigations.[85]

DOJ, in coordination with the FBI, other law enforcement agencies, and private entities, has success in pursuing botnet takedowns. The first successful takedown occurred in April 2011, when the government stopped "Coreflood" – an attack affecting more than 378,000 devices.[86] Since then, there have been other victories, including the recent takedown of two online black markets, AlphaBay and Hansa, with cooperation from foreign governments.[87]

Major Botnet Takedown Examples[88]

- 2011: DNS Changer[89]
- 2011: Coreflood (378,000 devices)
- 2013: Citadel (2 million devices)
- 2014: GameOver Zeus (500,000 to 1 million devices)
- 2016: Avalance (500,000 devices)
- 2017: Kelihos/Waldec (100,000 devices)

By reducing regulatory barriers that limit industry engagement, the government could more efficiently address even the most sophisticated of botnet attacks.

The government can enhance botnet takedowns by eliminating barriers that limit industry participation. Botnet takedowns require time, money, and resources, and few companies have the incentive to pursue legal action necessary to attempt a botnet takedown.[90] For industry, botnet takedowns typically involve assuming control of infrastructure, re-directing

[85] Raj Samani. McAfee, UK. *Briefing to the NSTAC ICR Subcommittee*. August 15, 2017.
[86] DOJ. "Department of Justice Takes Action to Disable International Botnet." April 13, 2011. https://www.justice.gov/opa/pr/department-justice-takes-action-disable-international-botnet.
[87] DOJ. "AlphaBay, the Largest Online 'Dark Market,' Shutdown." July 20, 2017. https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down.
[88] Leonard Bailey. DOJ. *Briefing to the NSTAC ICR Subcommittee*. August 10, 2017.
[89] http://www.dcwg.org/dns-changer/
[90] Ibid.

communications, and mitigating harms. Such activities frequently require either end-user authorization or a warrant, temporary restraining order, or civil injunction.[91] This is challenging when malicious attacks originate on outside of an ISP's own network. Thus, governments – together with industry support – are best positioned to lead botnet takedown activities.

Another issue potentially holding back take downs is measurements of success for prosecutors. In the context of criminal activity in the physical world, the government's goals and incentive structures reflect a focus on identifying and prosecuting defendants. Such traditional goals and incentive structures may not be fully optimized for the virtual world, which enables cyber criminals to have greater anonymity and therefore significantly frustrates efforts to identify and prosecute them as defendants. However, there are also other ways that prosecutors can disrupt and deter crime – including malware-enabled botnets attacks – in the virtual world. While continuing to seek and prosecute criminal defendants, which remains critical, prosecutors may also be incentivized to focus more broadly on crime prevention and national security. Prosecutors can help to prevent the proliferation and negative impact of botnets. They can disrupt and dismantle botnet operations, even when no potential defendant is discernible.

Disrupting and dismantling botnets can have significant positive impacts. For instance, public-private partnership efforts to sever ties between infected computers and the infrastructure of Citadel, one of the largest botnets documented, ceased 90 percent of the botnet's activity.[92] Likewise, the government's takeover of Coreflood, which used malicious software to siphon personal and financial information from unsuspecting users, allowed victims to remove the malicious software from their machines and prevented further loss of privacy and damage to users' financial security. Within nine days, the number of beacons from infected computers being sent to the servers decreased significantly.[93]

However, many botnets are not disrupted by the government – or there is a delay in their disruption – as, consistent with their incentive structure, many prosecutors are most focused on identifying and prosecuting a criminal defendant.[94] Under current guidelines, federal prosecutors are only encouraged to commence prosecution when they believe that the person's conduct constitutes a federal offense and that the admissible evidence will be sufficient to obtain and sustain a conviction. This focus on prosecutions limits the government's disruption and dismantlement of botnets because, in large part, there is not a readily identifiable person(s) to prosecute – even when crimes are ongoing.

The government has effectively increased its focus on prevention in other contexts; DOJ has effectively pivoted more resources and energy towards prevention in the counterterrorism context. Lessons learned from those successes may be applicable as the government considers how to evolve cybercrime-related incentive structures in a way that's not exclusively tied to

[91] See Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030); Wiretap Act (18 U.S.C. § 2511); Pen Register/Trap and Trace Statutes (18 U.S.C. §§ 3121 *et seq.*).

[92] Zach Lerner, *Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets*, 28 HARV. J.L. & TECH. 237, 247 (2014).

[93] Government's Supplemental Memorandum in Support of Preliminary Injunction, pg. 4, Figure 1 in *United States v. John Doe*, No. 3:11-cv-561 (VLB) (D. Conn. Filed Apr. 11, 2011).

[94] The United States Attorney's Office (USAO) annual budgets and performance measures are directly tied to number of convictions.

prosecutions and convictions, but rather encourages coordination across federal agencies and with the private sector on disrupting and dismantling botnets. For instance, while the FBI is vested with the important function of investigating cybercrimes, its authority to act is not without limitation. The FBI must cooperate, coordinate, and seek the approval of federal prosecutors to employ certain investigative tools, and authorization is usually withheld unless there is a likelihood of conviction, limiting the government's potential to prevent cybercrime and to protect against national security risks. Refocusing resource and incentive structures would also enable the government to leverage and partner with the private sector on cybercrime prevention more regularly and more productively to better protect botnet victims and increase the costs of botnet operations for criminals. Increasing the costs of criminal operations has a positive cascading effect; reducing the number of criminals who can afford to participate in online crime also reduces "noise" in the ecosystem, enabling both public and private sector entities to more effectively identify stealthier advanced persistent threats.

The NSTAC recommends the following actions to enhance take down efforts:

- **DOJ policies should be more supportive of government intervention. DOJ may need additional resources in order to increase these efforts which also are dependent upon collaboration with both the private sector and potential international partners.**

- **The national security implications of botnets justify a focus by DOJ on prevention and disruption of botnet attacks, not prosecutio**n.

- **The budget for cybercrime at the federal level should reflect the importance of prevention and should not be tied to prosecution and convictions.**[95]

Government must also ensure that existing law does not limit industry's information sharing or appropriate "active defense" activities. Statutes like the *Computer Fraud and Abuse Act*, the *Wiretap Act*, and *Pen Register/Trap and Trace Act* may unintentionally discourage ISPs from taking certain "active defensive measures" – such as implementing ingress/egress filtering (BCP 38 and 84), blocking reported bad traffic, and neutralizing a system that is attacking the provider's network – due to legal liability concerns.[96] There are limited legal protections for mistakes, and companies face potential criticism for errors. The government should look for ways to limit liability risks to providers who in good faith employ active defensive measures. The *Cybersecurity Information Sharing Act* (CISA) of 2015 authorizes monitoring of information on an information system for cybersecurity purposes and provides liability protections for such activities and other defensive measures.[97] Statutes like CISA allow industry to protect their networks and support government takedown efforts. If more is expected from the private sector, additional protections should be considered. Improved cybersecurity will require mutually beneficial partnership between industry and the government.

[95] Richard Boscovich. Microsoft. *Briefing to the NSTAC ICR Subcommittee*. August 16, 2017.

[96] Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030); Wiretap Act (18 U.S.C. § 2511); Pen Register/Trap and Trace Statutes (18 U.S.C. §§ 3121 *et seq.*); Leonard Bailey. DOJ. *Briefing to the NSTAC ICR Subcommittee*. August 10, 2017.

[97] Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, 129 Stat. 2242 (2015).

RECOMMENDATIONS

Efforts are underway to enhance accountability for agencies, as reflected by the President in EO 13800.[98] The government must build upon these efforts, leading by example. In addition, government must aggressively employ its law enforcement tools, while removing barriers to private action.

- **Set an Example by Sensibly Leveraging Capabilities in Procurement**. The government should invest in increasing the security of federal networks. Current efforts, such as the roll out of the Continuous Diagnostics and Mitigation for civilian agencies and Comply to Connect for the DoD, both rooted in NIST best practices, allow agencies to detect, inventory, and remediate all IoT and operational-technology devices, and Windows-based endpoints, on federal networks. Leadership in this area could set an example for private industry.

- **Employ NIST Standards and Guidance for Federal Information Security Management Act and IT Management**. NIST, working with the private sector, is continuously improving cybersecurity best practices. This includes efforts to enhance its framework, upgrade cryptographic capabilities (particularly quantum resistant cryptography), and explore AI and IoT security capabilities. NIST is also working to improve Internet architecture, including domain and BGP security. The government should be among the first to implement these standards.

- **Increase Law Enforcement Botnet Take Downs**. The government should leverage recent successes in botnet takedowns to demonstrate the effectiveness of prevention. Among other things, the government should consider:

    - Ensuring that incentive structures reflect the importance of prevention rather than being significantly tied to prosecution and convictions;

    - Streamlining law enforcement processes for botnet takedowns, including use of definitive sentencing guidelines;

    - Supporting public-private collaboration on takedowns; and

    - Modernizing its cyber-intelligence collection methods by allowing an analyst to focus on one target for a longer period, thus becoming an expert and more capable of combatting a specific attack. While considering ways to enhance botnet take downs, it is imperative that the government act transparently.

- **Avoid Duplication**. The government should consolidate and coordinate efforts to strengthen the Nation's cybersecurity more efficiently. For example, there have been several overlapping efforts to improve supply chain security from a variety of agencies including NIST, DHS, and the FCC. There have also been overlapping efforts for IoT security, including at DHS, NIST, and NTIA, as well as at multiple agencies who oversee the various IoT verticals (such as

[98] White House Office of the Press Secretary. *Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. May 16, 2017. https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

vehicles, Smart Cities etc.). These are important issues that would benefit from a coordinated approach.

- **Maintain a Convening and Promoting Role**. The government is uniquely equipped to convene industry to apply existing frameworks to new areas like IoT and develop best practices for evolving technologies. Multi-stakeholder processes, such as those at NIST and NTIA, should be encouraged and their practical advice promoted. Although the government should not issue mandates, it can encourage entities to adopt these standards by providing incentives. At the same time, the government needs to review the standards that emerge from these processes to identify and fill any gaps that could affect IoT.

- **Increase Protections for ISPs Pursuing Defensive Measures**. Existing statutes frequently discourage use of active defense measures by industry. The government should therefore look for ways to limit legal liability for providers seeking to protect their systems from botnet attacks.

- **Fund Research into Cybersecurity and Standards Development.** Funding for research and development is imperative. The government should financially support these efforts, including research of baseline path measurements, router-level topology, facility-level topology, performance, and security hygiene best practices. Research into new technologies – particularly quantum technology – is necessary as threats evolve and encryption becomes less effective.

- **Promote Voluntary Consensus Standards and Guidelines.** Public-private partnerships and voluntary guidelines are more effective than mandates, which quickly become obsolete in this ever-evolving environment.[99] Any regulation should focus on risk mitigation and limiting liability that may arise from industry efforts to share information and employ defense measures.

3.6 International

FINDINGS

No discussion of distributed attacks is complete without special attention to international actors, which are part of each ecosystem layer above. International influencers and challenges include:

- **International Technology Companies**. Device manufacturers and service providers span the globe, selling products internationally. This includes a diverse array of equipment manufacturers (such as smartphones, appliances, cars, industrial sensors, and medical devices) to global Internet and mobile service providers (mobile virtual network operators, network owners, ISPs, private network operators, wholesalers, and resellers).

- **Global Supply Chains**. Software, chipsets, and other components for IoT devices and the global communications networks come from around the world.

[99] Raj Samani. McAfee, UK. *Briefing to the NSTAC ICR Subcommittee.* August 15, 2017.

- **Internet Management Entities**. Various entities are involved in the core management and functions of the global Internet infrastructure from domain names to traffic routing. The Internet Corporation for Assigned Names and Numbers and numerous others participate in governance issues as well as day to day activities.

- **Individual Governments and Regional Blocks**. Each government has the same equities and roles as the United States: user/purchaser, regulator, and sovereign. Different countries have different approaches to technology regulation and policy. Regions have collaborated as well, with the Europeans and Asian nations working collectively on aspects of technology and Internet policy, including IoT. National and regional efforts feed into global systems and bodies.

- **Global Standards Bodies and Industry Cooperatives**. Dozens of standards bodies, from the Institute of Electrical and Electronics Engineers to the Alliance for Telecommunications Industry Solutions and ISO, shape international technology standards and protocols. Their work relies on consensus to promote true innovations in communications networking, including interoperability. They rely on the expertise and participation of an international community. Industry groups work together as well; examples include GSMA, the Telecommunications Industry Association, and others. And some regional groups, like the American Registry for Internet Numbers, are key to broader global communications networking.

Botnets are a global threat. Over 80 percent of botnet traffic originates overseas.[100] Addressing the botnet challenge requires international cooperation to develop standards, and all countries must work to secure their networks and devices.

United Kingdom Government Effort as One Example

Countries take varied approaches, but the most promising efforts include true partnerships between the private sector and government, free from fear of liability or recrimination. For example, the proactive work underway in the United Kingdom., which includes public awareness campaigns, internal government practices, and private-public partnerships has led to more secure networks.[101]

- **Public Awareness Campaigns**. The U.K. Government has launched a variety of public awareness campaigns aimed at educating the public about safer practices. It collaborated with large device manufacturers to push for two-factor authentication accounts, which lessen the security concerns related to stolen passwords. The government also uses its websites to remind users to upgrade their software. For example, tax filers who use out-of-date software to submit returns are warned to update their software and are unable to file if they do not update by the next filing period. The government is starting a partnership with academia to translate data and statistics about cyber security and hygiene into information and graphics

[100] Mike Bergman. Consumer Technology Association. *Briefing to the NSTAC ICR Subcommittee.* August 3, 2017 (stating that approximately 89% of the attacking locations for the Mirai/Dyn attack were located in a foreign country).

[101] Ian Levy. UK National Cyber Security Center. *Briefing to the NSTAC ICR Subcommittee.* August 9, 2017.

the public can understand. These important steps will help the public understand the importance of cybersecurity and take appropriate actions to change their behavior.

- **Internal Government Practices**. The United Kingdom protects its online footprint. It added domain-based message authentication, reporting and conformance to every government domain in the country to prevent email spoofing. To reduce malware attacks, the government performs an automatic scan of any site utilizing a gov.uk name. The government is also protecting the gov.uk branding by aggressively tracking and taking down websites spoofing.gov.uk websites. The government is also taking steps to better manage its enterprise. It collects data on which agencies are behind on updates and uses that to force system integrators to improve or risk the government publishing that information for public consumption. The government is also trying not to purchase software that is unsafe or that has not been validated.

- **Private-Public Partnerships**. Partnerships between the U.K. Government and the private sector helps prevent attacks and make networks more secure. For example, the government asked hosts to take down or fix harmful traffic, which resulted in a dramatic decrease in availability of phishing, webinject, and government-brand phishing. According to information provided by the U.K. Government Communications Headquarters (GCHQ) the government succeeded in taking down 153 phishing kit credential stores, 2570 advanced fee fraud attacks, and 23,000 mail relays. To protect its networks, the government built a public-sector scale recursive DNS structure that includes a filtering service. It offers this service to ISPs for free. According to GCHQ, as of July 2017, this service has blocked 23,046 unique domains hosting malicious content. Use of the government's phishing and malware mitigation service resulted in 79,567 attacks successfully taken down. The government is also using a "name and shame" tactic to encourage industries like banks and ISPs to incorporate secure processes in their defenses.

Other International Partnerships

In Europe, the "No More Ransom" project is a collaboration between the European Cybercrime Center, Dutch police, and commercial companies including Amazon Web Services.[102] The initiative was created to serve as a single repository of encryption keys with the purpose of improving global security. The community informs victims of what ransomware they have been infected with and has collectively taken down various malware including Shade, Chimera, and WildFire. This initiative also provides 50 publicly available encryption tools for ransomware victims. Efforts like "No More Ransom" are important steps for the international community to take to fight botnets.

RECOMMENDATIONS FOR GOVERNMENT

- **The U.S. Government Should Develop International Norms that Will Slow Botnet Proliferation.** The United Kingdom shows that governments can play an important role in modeling security and working with the private sector to make networks – private and public – more secure. Other governments can learn from this example; however, governments

[102] Raj Samani. McAfee, UK. *Briefing to the NSTAC ICR Subcommittee.* August 15, 2017.

cannot act alone. The U.S. Government should collaborate with the private sector to work within international standards bodies to develop standards modeled after best practices to guide governments and service providers. Widespread adoption of standards will provide an important defense.

- **The U.S. Government Should Drive Towards an International Framework for Device Security**. Developing secure devices requires international cooperation. This includes identification of a body or bodies that could be stewards of developing a framework or platform for information sharing on device security features and behavioral fingerprints and/or patching and upgradeability requirements. These standards can help manufacturers develop more secure devices and help enterprises and consumers better manage their devices.

- **Develop International Deterrence Against Nation State Attacks.** Nation states now originate a significant number of botnet attacks. Deterring this behavior will require international bodies and individual nations to take a hard stance against such actions. These actions will eliminate a significant source of these attacks and, more importantly, start to raise the cost for the attackers.

4.0 CYBER SECURITY MOONSHOT

The preceding section of this Report (*Section 3.0*) focused on short-term recommendations related to existing, known best practices and technologies that, if implemented more broadly, could have an immediately tangible impact on reducing the threat of automated and distributed cyber attacks. The NSTAC ICR Subcommittee's findings reinforced the NSTAC's previous recommendation in the *NSTAC Report to the President on Emerging Technologies Strategic Vision*[103] that the Nation's current cybersecurity challenges are not primarily limited by the technological environment but by human-controlled factors, such as various legal, behavioral, and educational challenges that have thus far limited the deployment of widely accepted cybersecurity best practices.

While full implementation of the recommendations in *Section 3.0* would have a tangible impact on the Nation's cybersecurity, these collective recommendations ultimately still represent incremental solutions that are insufficient in addressing the totality of the Nation's more fundamental and persistent cybersecurity challenges. Further, the NSTAC has concluded that the current and emerging technology landscape – including significant advances in machine learning, cloud, and quantum computing – provides the requisite enabling foundation to achieve a dramatic transformation in cybersecurity. The NSTAC determined that efforts are primarily missing a concerted national unity of effort and strategic direction. As such, the NSTAC reiterates its recommendation, first referenced in the *NSTAC Report to the President on Emerging Technologies Strategic Vision*, that the government establish a national cybersecurity Moonshot.

[103] NSTAC. *NSTAC Report to the President on Emerging Technologies Strategic Visions,* https://www.dhs.gov/sites/default/files/publications/Draft%20NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20%287-10-17%29%20v3%20%281%29-%20508.pdf

With the endorsement of the White House, the NSTAC commits to initiating the cybersecurity Moonshot concept to provide private industry advice on how the government could most effectively coordinate a national effort. Based on the consensus of the NSTAC and EOP, this study would be time bound to reflect both the short-term urgency of the cybersecurity challenge, while ensuring a thoroughness and rigor appropriate for an initiative of this magnitude. In conducting this study, the NSTAC proposes an initial two-fold course of action.

Defining the Process: Core Principles of Moonshot Models

The first phase of the NSTAC study will review successful models, irrespective of industry or subject matter, that generally reflect core principles of Moonshot efforts. The NSTAC will look well beyond the cybersecurity domain to identify lessons learned from previously successful national mobilization efforts. This first phase of study will be focused on answering the fundamental question: *What are the core, defining principles consistent across successful Moonshot models?*

As a starting basis, the NSTAC will focus on identifying other initiatives characterized by the principles listed below. These proposed elements are only guidelines to inform the initial scope of study and would not be considered comprehensive. As of the time of this writing, it is the NSTAC's conclusion that for an effort to qualify as a Moonshot, it must be characterized by at least the following elements:

- **National Call to Action:** The government, at the senior-most levels, must publicly deem an issue of significant national consequence and declare its solution a national strategic priority.

- **End-Goal Focused**: The government must emphasize a strategic vision oriented toward the ambitious end goal, with a defined time-based deadline, without prescriptively defining the incremental steps necessary towards achieving that end goal.

- **Multi-Stakeholder Process:** The government must catalyze the national effort by leveraging its unique convening authorities and creating the appropriate collaborative mechanisms required to formally leverage the multi-stakeholder community, including at least private industry and academia, to execute against the defined strategic end goal.

Specifically Defining the Cybersecurity Moonshot

The second phase of the NSTAC study will focus on applying the domain-agnostic lessons learned from these national Moonshot efforts to the cybersecurity domain. This second phase will seek to provide further clarity and recommendations on key cybersecurity considerations related to the identified Moonshot principles (Call to Action, End-Goal Focus, and Multi-Stakeholder Process), and others yet to be identified. As such, in this second phase of the study, the NSTAC will hear from a variety of cybersecurity experts and others to appropriately define the stated end goal, and the sub-elements of the end goal. This phase will seek to answer the question: *What is an appropriately scoped moonshot, applied to the cybersecurity domain?*

5.0 GOVERNMENT MUST COLLABORATE WITH INDUSTRY

The government must lead in addressing cybersecurity threats to our connected, digital future. Threats come from nation-states, organized crime, hacktivists, terrorists, and others. The private sector cannot do it alone. The Federal Government must lead at home and abroad, by fostering collaboration across economic sectors and political borders. The NSTAC recommends the following activities that the government must do to address IoT security.

Protect and Expand Public-Private Partnerships, Which Have Been the Bedrock of Federal Cyber Policy. Industry has partnered with DHS in venues like the NCCIC and U.S. Computer Emergency Readiness Team for decades. Industry also works with the government in the CSRIC, Technology Advisory Council, and other settings, including NIST and NTIA.

Industry has collaborated with the government to protect critical infrastructure. In response to EO 13636, which called for the identification and protection of critical infrastructure, eight Financial Sector Chief Executive Officers initiated an effort to enhance cybersecurity of core financial services known as the Financial Systemic Analysis and Resilience Center (FSARC). FSARC, in collaboration with the government, coordinates campaigns against key adversaries, develops and shares best practices and lessons learned, contributes to criminal cases in support of federal law enforcement, and leverages U.S. Government access and information to identify where criminal activity is aligned with or utilized by foreign intelligence actors.[104] The private sector helped shape, and has been implementing the NIST's Cybersecurity Framework and sectors have been mapping it to their unique needs. For example, CSRIC IV's March 2015 final document, *Cybersecurity Risk Management and Best Practices*,[105] provides guidance to help communications providers use and adopt the NIST Cybersecurity Framework. Initiatives like this are particularly helpful for smaller providers operating within constrained budgets.

Such partnerships rely on trust and must remain free from the threat of regulation and enforcement.

Consider Creative Ways to Cultivate Information Sharing About Vulnerabilities, Including Liability Protections and Safe Harbors. If operators and manufacturers are going to discuss product and service vulnerabilities, there must be a recognition of the risks associated with doing so, and protection for such activity. Vulnerability disclosure programs are interesting, but may lack key components to work. In 2016, DHS noted that it should convene a group of partners to consider liability, among other issues.[106] The U.S. Chamber Institute for Legal Reform and others have been looking at these issues, for example, in *Torts of the Future*, the Chamber notes that "[m]anufacturers of connected products face significant liability risks stemming from

[104] Scott DePasquale. Financial Services Analysis & Response Center. *Briefing to the NSTAC ICR Subcommittee.* August 10, 2017

[105] FCC, CSRIC IV, Working Group 4: Final Report, *Cybersecurity Risk Management and Best Practices Working Group*. March 2015.https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[106] See DHS. "Strategic Principles for Securing the Internet of Things (IoT)." Version 1.0. November 15, 2016. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.

cyberattacks or the theft of private information."[107] The Federal Government must consider how civil litigation risk and our litigious judicial system can hinder beneficial activity.

Identify and Address Legal Limits That Constrain Private Sector Defensive Measures. DDoS and other mitigations may expose companies to risk under federal law. They may also have unintended consequences such as harm to third parties if there are errors in attribution. The government must identify its goals for active defense and the role of the private sector. Additionally, the government must consider whether the protections and authorities in CISA are enough. Protection for sharing cyber threat indicators and defensive measures [108] may not be enough. Appropriate liability protection for ISPs and others will be critical in further developing defensive measures and information sharing. Liability protection legislative language must be updated lockstep with any expanded role for members of the ecosystem.

Adjust How U.S. Intelligence Operates When Addressing Cyber Threats. The National Infrastructure Advisory Council (NIAC) recently evaluated the United Kingdom and Israel's approaches to intelligence gathering.[109] The NIAC suggests that "effective coordination at speed, is driven by a central authority that can coordinate cyber priorities for the nation, align industry and government resources and provide national leadership for cyber defense."[110] The report further discusses the efforts in the United Kingdom in creating the U.K. National Cyber Security Centre and the Israeli National Cyber Bureau. The NSTAC recommends that the U.S. Government evaluate these models and determine if any of the concepts under development in the United Kingdom and Israel may be helpful in organizing U.S. Government cybersecurity efforts. The NSTAC also recommends that the United States should consider altering its cyber intelligence collection methods by allowing an analyst to solely focus on one target for a longer period, thus becoming an expert and possibly more capable of combatting a specific attack from their target.

Improve Information Sharing with the Private Sector. The government has access to intelligence information; however, the process for sharing that information at the classified level can be cumbersome. The NSTAC recommends that the President direct the Federal Government to conduct a review of existing information programs to determine if they are meeting objectives and recommend new approaches, even on a pilot basis, to enable better information sharing. The government should also acknowledge that not all recipients of information have the same capabilities. There should be a range of information sharing models available commensurate with the abilities of each party.

Eliminate Regulatory Overhang at The Federal, State, and Local Levels. The private sector is concerned about regulatory obligations, technical mandates, and reporting regimes that will

[107] U.S. Chamber Institute for Legal Reform. "Torts of the Future—Addressing the Liability and Regulatory Implications of Emerging Technologies." March 2017. http://www.instituteforlegalreform.com/uploads/sites/1/_Torts_of_the_Future_Addressing_the_Liability_and_Regulatory_Implications_of_Emerging_Technologies_April_2017.pdf?pagename=uploads/sites/1/Torts_of_the_Future_Addressing_the_Liability_and_Regulatory_Implications_of_Emerging_Technologies_.pdf.

[108] Section 104(c) of the Cyber and Information Sharing Act of 2015, 6. U.S.C. 1504.

[109] NIAC. "Securing Cyber Assets—Addressing Urgent Cyber Threats to Critical Infrastructure." August 2017. https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf.

[110] NIAC Report to the President "Securing Cyber Assets," at 19 (August 2017), available at https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf

use up valuable resources and encourage a compliance mindset that will prioritize a "check the box" mentality instead of nimble and aggressive innovation. In the cybersecurity space, threats, vulnerabilities, and responses move exponentially faster than any regulator could. If the government wants true partners, it must make clear that collaboration and best efforts will not rebound on the private sector in regulation and punitive enforcement. The Federal Government should discourage state activity, whether in technical mandates, online privacy burdens, or other measures, as they can complicate and hinder product and service development.

The government may recognize that there is, and will continue to be, state activity, whether in technical mandates, online privacy burdens, or other measures, and that some of these efforts can fragment and complicate product and service development. Given this reality, the NSTAC recommends that the Federal Government encourage states first to adopt and implement available consistent cybersecurity best practices and recommendations for the states' own administrative organizations and systems and then to promote the same for the states' resident and business ecosystem. States should be encouraged to participate in national venues with key stakeholders to attain consistent approaches toward cybersecurity. These should include the National Governors Association, the National Association of State Chief Information Officers; the National Conference of State Legislatures, and the DHS State, Local, Tribal, and Territorial Government Coordinating Council.

Aggressively Represent U.S. Policy and Economic Interests Abroad. The global ICT sector needs the U.S. Government to lead abroad. Regions and countries are addressing security and technology in divergent ways. It is a matter of national security and economic interest that the United States vigorously champion open markets, technological neutrality, and transparent standards processes. If the United States does not lead, other nations' legal standards and prescriptive regulations could set international benchmarks and slow U.S. companies' international growth.

Promote Cybersecurity Workforce Development. Numerous reports recommend that the government address cyber workforce deficiencies that may cripple our ability to respond to expanding threats. Examples include the NIAC Report (suggesting a public-private expert exchange program, for example),[111] CSRIC's Final Report, *Cybersecurity Workforce Development Best Practices Recommendations*,[112] various DHS efforts, including the establishment of the National Initiative for Cybersecurity Careers and Studies,[113] the National Cybersecurity Workforce Framework,[114] the Cybersecurity Workforce Development Toolkit,[115]

[111] NIAC. "Securing Cyber Assets—Addressing Urgent Cyber Threats to Critical Infrastructure." Recommendation 4. August 2017. https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf.

[112] CSRIC. WG7 Final Report. "Cybersecurity Workforce Development Best Practices Recommendations." March 2017. https://www.fcc.gov/files/csric5-wg7-finalreport031517pdf.

[113] NICCS, https://niccs.us-cert.gov/.

[114] NICCS. NICE Cybersecurity Workforce Framework. https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.

[115] NICCS. "Cybersecurity Workforce Development Toolkit—How to Build a Strong Cybersecurity Workforce." March 2017. https://niccs.us-cert.gov/sites/default/files/documents/pdf/cybersecurity_workforce_development_toolkit.pdf?trackDocs=cybersecurity_workforce_development_toolkit.pdf.

and the Report on Improving Cybersecurity in the Health Care Industry[116] (June 2016). In addition, cybersecurity personnel may need to understand both coding and foreign languages, as most botnets are coded using languages other than English. There is much work to be done, but a consensus has emerged that this is a critical area for government attention.

Take Care in Using the Procurement System to Address Cybersecurity for IoT. The government should be thinking about how to ensure that its products and services are appropriately secured. However, the government should avoid disproportional focus on the devices or relying on one-sided mandates to achieve this enhanced security. The NSTAC recommends that the government explore Managed Services that can be offered by experts in the private sector. This would enable the government to harness the expertise and scale of the private sector (ISPs, cloud providers, others that provide services to third parties) rather than using more rudimentary device security mandates.

Develop Think Tanks to Explore Moonshot Opportunities. Instead of repeating previously attempted ideas such as extending new IP protocol, the government should identify new approaches. The NSTAC recommends that government explore the creation of collaborative and innovative partnerships and think tanks akin to NIST's National Cybersecurity Center of Excellence, which partners with the private sector, academia, and other agencies to find solutions to technology problems. Another approach to consider is a structure similar to cyber-focused Defense Advanced Research Projects Agency, which benefits from special statutory hiring authorities and alternative contracting vehicles that let the agency take advantage of opportunities to advance its mission.

6.0 CONCLUSION

Botnets and the attacks they facilitate are only expected to grow. Mitigating this complex problem will require a variety of actions from across the Internet ecosystem. While this Report provides recommendations for device makers, network service providers, software developers, enterprises, and the government, they are not the only entities that must be involved in mitigating the threat. Cybersecurity is a shared responsibility and dependent upon each part of the ecosystem playing a role. The NSTAC also expects that the range of solutions will evolve over time. Thus, the NSTAC does not anticipate that this Report or any successor processes will be static. Addressing this challenge will require ongoing collaboration and commitment between the private sector and the government. Finally, many of the recommendations are iterative and will not fundamentally change the underlying nature of the problem. For this reason, the NSTAC recommends that a future study of the NSTAC investigate the possibility of a cybersecurity Moonshot intended to target the underlying internet infrastructure and recommend long-term improvements.

[116] Health Care Industry Cybersecurity Task Force (HCIC Task Force). "Report on Improving Cybersecurity in the Health Care Industry." Recommendation 6.4. June 2017. https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

APPENDIX A: MEMBERSHIP

SUBCOMMITTEE MEMBERS

Mr. Raymond Dolan, Sonus Networks Inc., and Subcommittee Co-Chair
Mr. John Donovan, AT&T Inc., and Subcommittee Co-Chair

Mr. Chris Boyer, AT&T Inc., and ICR Working Group Co-Chair
Mr. Kevin Riley, Sonus Networks Inc. and ICR Working Group Co-Chair

AT&T, Inc.	Mr. Jonathan Gannon Mr. Bill O'Hern
Avaya, Inc.	Mr. Vico Loquerico
CenturyLink, Inc.	Ms. Kathryn Condello Mr. Paul Diamond Mr. John Schiel Mr. Donald Smith
Communication Technologies, Inc.	Mr. Milan Vlajnic
Department of Homeland Security	Mr. Gregory Shannon
Diogenes Group, LLC	Mr. William Gravell
Dun & Bradstreet Corporation	Mr. Gregory Mortensen Mr. Jon Rose
Equinix, Inc.	Ms. Cindy Liu
ForeScout Technologies, Inc.	Mr. Tamer Baker Ms. Katherine Gronberg
Lockheed Martin Corporation	Mr. Darrell Durst
Microsoft Corporation	Mr. Richard Boscovich Ms. Amanda Craig Deckard
McAfee, LLC	Mr. Patrick Flynn Mr. Kent Landfield
National Security Agency	Ms. Cheri Caddy
National Telecommunications and Information Administration	Mr. Shawn Cochran Ms. Megan Doscher

	Ms. Evelyn Remaley
National Institute of Standards and Technology	Mr. Tim Polk
NCTA – The Internet & Television Association	Mr. Matt Tooley
Neustar, Inc.	Ms. Terri Claffey
Oracle Corporation	Dr. Prescott Winter
Palo Alto Networks, Inc.	Mr. Sean Morgan
Raytheon Company	Mr. Michael Daly
Unisys Corporation	Mr. Mark Cohn Mr. Tom Patterson
USTelecomm	Mr. Robert Mayer
Verizon Communications, Inc.	Mr. Kevin Kirsche Mr. Timothy Vogel

BRIEFERS – SUBJECT MATTER EXPERTS

Arbor Networks, Inc.	Ms. Arrabelle Hallawell
AT&T, Inc.	Mr. Brian Rexroad Mr. Bill O'Hern
CA Technologies, Inc.	Mr. Jaime Brown
Center for Democracy and Technology	Ms. Michelle Richardson
Consumer Technology Association	Mr. Mike Bergman
Cyber Threat Alliance	Mr. Michael Daniel
Department of Defense	Mr. Mitchell Komaroff
Department of Homeland Security	Dr. Ann Cox
Department of Justice	Mr. Leonard Bailey
Dun & Bradstreet Corporation	Dr. Anthony Scriffignano
Embassy of Japan	Mr. Daisuke Hayashi

Federal Bureau of Investigation	Mr. Tom Grasso
ForeScout Technologies, Inc.	Mr. Wallace Sann
Financial Services Analysis & Response Center	Mr. Scott DePasquale
Financial Systematic Analysis & Resilience Center	Mr. Bill Nelsen
Japanese Ministry of Internal Affairs & Communication	Mr. Atsushi Goto Mr. Yasu Taniwaki
Japanese National Center of Industry Readiness and Strategy for Cybersecurity	Ms. Kasumi Sugomoto
Intelligence Advanced Research Project Agency	Mr. Kerry Long
McAfee United Kingdom	Mr. Raj Samani
Micron Technology, Inc.	Mr. Steve Wallach
Microsoft	Mr. Richard Boscovich Mr. Rob Spiger
NCTA – The Internet & Television Association	Mr. Matt Tooley
National Security Agency	Ms. Cheri Caddy
National Institute of Standards and Technology	Mr. Andrew Regenscheid Dr. Charles Romine
Neustar, Inc.	Mr. Barrett Lyon
Oracle	Mr. Travis Russell
Palo Alto Networks, Inc.	Mr. Kevin Walsh
Raytheon Company	Mr. J.F. Mergen
sn3rd LLC	Mr. Sean Turner
Unisys Corporation	Mr. Brent Houlahan Mr. Jack Koons
United Kingdom Nation Cyber Security Centre	Dr. Ian Levy
US Marine Corps	Dr. Ray Letteer

USTelecom	Mr. Robert Mayer
Venable LLP	Mr. Ari Schwartz
VeriSign, Inc.	Mr. Danny McPherson Dr. Eric Osterweil

SUBCOMMITTEE MANAGEMENT

NSTAC Designated Federal Officer	Ms. Helen Jackson
Alternate NSTAC DFO	Ms. Sandy Benevides Ms. DeShelle Cleghorn
Booz Allen Hamilton, Inc.	Ms. Ursula Arno Mr. William Hyde
Total Systems Technology Corporation	Mr. Robert Carter

APPENDIX B: ACRONYMS

5G	Fifth Generation
ABC	Anti-Botnet Code of Conduct
AI	Artificial Intelligence
BCP	Best Common Practices
BGP	Border Gateway Protocol
BYOD	Bring Your Own Device
CharGen	Character Generator Protocol
CISA	Cybersecurity Information Sharing Act
CITL	Cybersecurity Independent Testing Laboratory
CNSSI	Committee on National Security Systems Instruction
CSRIC	Communications Security, Reliability and Interoperability Council
CTA	Consumer Technology Association
CVD	Coordinated Vulnerability Disclosure
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DOC	Department of Commerce
DoD	Department of Defense
DOJ	Department of Justice
DoS	Denial of Service
EO	Executive Order
EOP	Executive Office of the President
ETSV	Emerging Technology Strategic Vision
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FSARC	Financial Systemic Analysis and Resilience Center
FTC	Federal Trade Commission
Gbps	Gigabits Per Second
GCHQ	Government Communications Headquarters
GSMA	Groupe Spécial Mobile Association
ICR	Internet and Communications Resilience
ICS	Industrial Control System
ICT	Information and Communications Technologies
IEC	International Electrotechnical Commission
IETF	Internet Engineering Technical Forum
IoT	Internet of Things
IP	Internet Protocol
IPv6	Internet Protocol Version 6
ISO	International Organization for Standardization
ISP	Internet Service Providers
IT	Information Technology
M2M	Machine to Machine
M3AAWG	Messaging, Malware, and Mobile Anti-Abuse Working Group

MUD	Manufacturer Usage Description
NCCIC	National Cybersecurity and Communications Integration Center
NCCoE	National Institute of Standards and Technology National Cybersecurity Center of Excellence
NFV	Network Functions Virtualization
NIAC	National Infrastructure Advisory Council
NIST	National Institute of Standards and Technology
NISTIR	NIST Glossary of Information Security Terms
NMD	Network Monitor Devices
NS/EP	National Security/Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee
NTIA	National Telecommunications and Information Administration
NTP	Network Time Protocol
OS	Operating System
RPKI	Resource Public Key Infrastructure
SAFECode	Software Assurance Forum for Excellence in Code
SDL	Security Development Lifecycle
SDN	Software Defined Network
SS7	Signaling System 7
U.K.	United Kingdom
UL	Underwriters Lab
U.S.	United States
VPN	Virtual Private Network

APPENDIX C: GLOSSARY

5G – A future, fifth generation mobile network, whose specification the International Telecommunications Union has not been fully defined. It is expected to support 10 gigabits per second data rates and higher. Commercial 5G deployments are not expected until around 2020. (Newton's Telecom Dictionary)

Artificial Intelligence – The intelligence exhibited by machines or software. A term popularized by Alan Turing, it historically describes a machine that could trick people into thinking it was a human being via the Turing Test. Recently, scientists within this field largely have abandoned this goal to focus on the uniqueness of machine intelligence and learn to work with it in intelligent, useful ways. (Newton's Telecom Dictionary)

Authentication – The process whereby a user, information source, or simply information proves they are who they claim to be; the process of determining the identity of a user attempting to access a network and/or computer system. (Newton's Telecom Dictionary)

Botnet – A network of Internet-connected computers that have been infected by a malicious third-party's command-and-control software and are able to be remotely instructed by that third party to perform harmful actions such as launch attacks over the Internet. (Newton's Telecom Dictionary)

Cloud Computing – A model for enabling on-demand network access to a shared pool of configurable information technology capabilities/resources, (for example, networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. Both the user's data and essential security services may reside in and be managed within the network cloud. (Committee on National Security Systems Instruction (CNSSI) 4009, Adapted) (NSTAC Report 2016)

Critical Infrastructure – System and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. Critical infrastructure can be owned and operated by both the public and private sector. [*Critical Infrastructures Protection Act of 2001*, 42 U.S.C. 5195c(e)] (CNSSI 4009, Adapted)

Cyber Attack – An attack, via cyberspace, targeting an enterprise's use of cyberspace for disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. (CNSSI 4009)

Cybersecurity – The ability to protect or defend the use of cyberspace from cyber attacks. (CNSSI 4009)

Denial of Service Attacks – The prevention of authorized access to resources or the delaying of time-critical operations. Time-critical may be milliseconds or it may be hours, depending upon the service provided. (CNSSI 4009)

Distributed Denial of Service Attacks – A denial of service technique that uses numerous hosts to perform the attack and prevents the authorized access to resources or delays time-critical operations. (NIST Glossary of Information Security Terms – (NISTIR) 7298 – Revision 2)

Firewall – A piece of hardware or software, or hardware and software, that prevents unauthorized people from gaining access to a computer or computer network. (Newton's Telecom Dictionary)

Internet of Things – The total interconnected collection of device networks. (Newton's Telecom Dictionary)

Internet Protocol (IP) – Part of the Transmission Control Protocol/IP family of protocols describing software that tracks the Internet address of nodes, routes outgoing messages, and recognizes incoming messages. It is also used in gateways to connect networks at Open Systems Interconnection Network Level 3 and above. (Newton's Telecom Dictionary)

Malware – Software created and distributed for malicious purposes, such as invading computer systems in the form of viruses, worms, or other plug-ins and extensions that mask other destructive capabilities. (Newton Telecom Dictionary)

National Security/Emergency Preparedness (NS/EP) Communications – Telecommunication services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States (47 Code of Federal Regulations Chapter II, § 201.2(g)). NS/EP communications include primarily those technical capabilities supported by policies and programs that enable the Executive Branch to communicate at all times and under all circumstances to carry out its mission essential functions and to respond to any event or crisis (local, national, or international), to include communicating with itself; the Legislative and Judicial branches; state, territorial, tribal, and local governments; private sector entities; as well as the public, allies, and other nations. NS/EP communications further include those systems and capabilities at all levels of government and the private sector that are necessary to ensure national security and to effectively manage incidents and emergencies. (NS/EP Communications Executive Committee definition based on Executive Order 13618, *Assignment of National Security and Emergency Preparedness Communications Functions* [2012])

Networks – Information system(s) implemented with a collection of interconnected components, which may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. (NIST Glossary of Information Security Terms (NISTIR) 7298 – Revision 2)

Network Virtualization – A means of improving the efficiency of a network and reducing costs. It involves creating multiple virtual partitions on a single piece of hardware. It cuts down on the

amount of network hardware required and allows multiple functions to be managed from a single console. (Newton's Telecom Dictionary)

Protocol – A set of rules and formats, semantic and syntactic, permitting information systems to exchange information. (NIST Glossary of Information Security Terms – NISTIR 7298 – Revision 2)

Software Defined Network – A virtual private network. Specifically, it refers to AT&T's Software Defined Network Service, which was introduced in 1985 for AT&T's largest customers and provided only dedicated access services. (Newton's Telecom Dictionary)

Threat – Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (NIST SP 800-53, CNSSI 4009, Adapted)

APPENDIX D: BIBLIOGRAPHY

AT&T. *Network Practices*. April 24, 2017. https://www.att.com/gen/public-affairs?pid=20879.

Arbor Networks. *Worldwide Infrastructure Security Report,* Volume XII, available at https://www.arbornetworks.com/insight-into-the-global-threat-landscape

Bailey, Leonard. DOJ. *Briefing to the NSTAC ICR Subcommittee*. August 10, 2017.

Bergman, Mike. CTA. *Briefing to the NSTAC ICR Subcommittee*. August 3, 2017.

Boscovich, Richard. Microsoft. *Briefing to the NSTAC ICR Subcommittee*. August 16, 2017.

Boyer, Chris. M3AAWG Public Policy Co-Chair (AT&T), *New M3AAWG Bot Metrics Report Shares Network Operators' Perspective*. October 20, 2014. https://www.m3aawg.org/blog/new-m3aawg-bot-metrics-report-shares-network-operators%E2%80%99-perspective.

Burke, Samuel. CNN. *Chinese Firm Acknowledges Inadvertent Role in Cyberattack.* October 24, 2016. http://money.cnn.com/2016/10/23/technology/ddos-cyber-attack-chinese-firm/index.html.

Cisco. *Cisco Visual Network Index: Forecast and Methodology, 2016-2021, White Paper*. June 7, 2017. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html.

Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030); Wiretap Act (18 U.S.C. § 2511); Pen Register/Trap and Trace Statutes (18 U.S.C. §§ 3121 *et seq.*); Leonard Bailey. *Briefing to the NSTAC ICR Subcommittee*. August 10, 2017.

Computer Weekly, "Global Hacker Botnet Tops 6 Million Hijacked Devices", September 27, 2017 http://www.computerweekly.com/news/450427023/Global-hacker-botnet-tops-6-million-hijacked-devices.

Consumer Technology Association, *Project Overview: Securing Connected Devices for Consumers in the Home, CTA-CEB33*, July 7, 2017. https://standards.cta.tech/apps/group_public/project/details.php?project_id=429.

Cox, Ann. DHS. *Briefing to the NSTAC ICR Subcommittee.* August 1, 2017.

Cyber Independent Testing Lab (CITL). http://cyber-itl.org/.

Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, 129 Stat. 2242 (2015).

CSRIC. WG7 Final Report. "Cybersecurity Workforce Development Best Practices Recommendations." March 2017. https://www.fcc.gov/files/csric5-wg7-finalreport031517pdf.

Department of Defense (DoD). "DOD Announces Digital Vulnerability Disclosure Policy and "Hack the Army Kick-Off." *Press Release*. November 21, 2016. https://www.defense.gov/News/News-Releases/News-Release-View/Article/1009956/dod-announces-digital-vulnerability-disclosure-policy-and-hack-the-army-kick-off/.

Department of Health and Human Services (HHS). "Postmarket Management of Cybersecurity in Medical Devices—Guidance for Industry and Food and Drug Administration Staff." December 28, 2016. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

Department of Homeland Security (DHS). "Strategic Principles for Securing the Internet of Things (IoT)." Version 1.0. November 15, 2016. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.

DHS. United States Computer Emergency Readiness Team. *Build Security In.* https://www.us-cert.gov/bsi.

Department of Justice (DOJ), *A Framework for a Vulnerability Disclosure Program for Online Systems* July 2017. https://www.justice.gov/criminal-ccips/page/file/983996/download.

DOJ. "AlphaBay, the Largest Online 'Dark Market,' Shutdown." July 20, 2017. https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down.

DOJ. "Department of Justice Takes Action to Disable International Botnet." April 13, 2011. https://www.justice.gov/opa/pr/department-justice-takes-action-disable-international-botnet.

ETSI NFV Industry Specialization Group. *Network Operators Perspectives on NFV Priorities for 5G.* February 21, 2017. https://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf

Ericsson Mobility Report. *On the Pulse of the Networked Society.* June 2016. https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf.

Federal Communications Commission (FCC), Communications Security Reliability and Interoperability Council (CSRIC) III, *U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers*, March 2012. https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf.

FCC, CSRIC II, Working Group 2A: Final Report, *Cyber Security Best Practices*. March 2011. https://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf.

FCC, CSRIC IV, Working Group 4: Final Report, *Cybersecurity Risk Management and Best Practices Working Group*. March

2015.https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

FCC CSRIC V, Working Group 5 Final Report, *Information Sharing*, March 15, 2017. https://www.fcc.gov/files/csric5-wg5-finalreport031517pdf.

FCC CSRIC. Working Group 7 Final Report, *Cybersecurity Workforce Development Best Practices Recommendations.* March 2017. https://www.fcc.gov/files/csric5-wg7-finalreport031517pdf.

FCC CSRIC V, Working Group 10, Legacy Risk Reductions (2017) (Legacy Risk Reductions Report), https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf.

Fitzgerald, Brian and Chris Wysopal. Veracode. *Briefing to the NSTAC ICR Subcommittee.* August 1, 2017.

Federal Trade Commission (FTC). "Announces Winner of its Internet of Things Home Device Security Contest." *Press Release*. July 26, 2017. https://www.ftc.gov/news-events/press-releases/2017/07/ftc-announces-winner-its-internet-things-home-device-security.

FTC. "FTC Approves Final Order Settling Charges Against TRENDnet. Inc." *Press Release*. February 7, 2014. https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc; https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.

FTC. Internet of Things: Privacy & Security in a Connected World. n.130. January 2015. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

FTC. IoT Home Inspector Challenge. 2017. https://www.ftc.gov/iot-home-inspector-challenge.

FTC. Staff Report. *Internet of Things: Privacy & Security in a Connected World, FTC*. January 2015. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

Franceschi-Bicchierai, Lorenzo, *How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet*. September 29, 2016. https://motherboard.vice.com/en_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs.

George Washington University, Center for Cyber and Homeland Security. *Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats.* October 2016. https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf.

GSA. Vulnerability Disclosure Policy. https://18f.gsa.gov/vulnerability-disclosure-policy/.

GSMA. IoT Security Guidelines. February 2016. https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/.

Hallawell, Arrabelle. Arbor Networks, Inc. *Briefing to the NSTAC ICR Subcommittee*. August 3, 2017.

Hartnett, Kevin. WIRED. *Computer Scientists Close in on Perfect, Hack-Proof Code.* September 23, 2016. https://www.wired.com/2016/09/computer-scientists-close-perfect-hack-proof-code/.

Health Care Industry Cybersecurity Task Force. *Report on Improving Cybersecurity in the Health Care Industry*. June 2017. https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

I Am the Cavalry. *DOT Gov Coordinated Disclosure Timeline*. https://www.iamthecavalry.org/wp-content/uploads/2016/12/IATC_Gov-Coordinated-Disclosure-Timeline_v1.0.jpg.

Incapsula. *Global DDoS Threat Landscape.* https://www.incapsula.com/ddos-report/ddos-report-q1-2017.html.

Koeberl, Patrick, et, al. "TrustLite: A Security Architecture for Tiny Embedded Devices." http://www.icri-sc.org/fileadmin/user_upload/Group_TRUST/PubsPDF/trustlite.pdf

Lerner, Zach, "Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets," 28 HARV. J.L. & TECH. 237, 247 (2014).

Letteer, Ray. U.S. Marine Corps. *Briefing to the NSTAC ICR Subcommittee*. August 30, 2017.

Levy, Ian. UK National Cyber Security Centre. *Briefing to the NSTAC ICR Subcommittee.* August 9, 2017.

McAfee. *Mirai IoT Botnet Attack: A Honeypot Illustration.* April 5, 2017. https://www.youtube.com/watch?v=vnitAXYGmI0.

McAfee. Secure Home Platform Service. https://securehomeplatform.mcafee.com/.

Microsoft. What is the Security Development Life Cycle? https://www.microsoft.com/en-us/sdl/default.aspx.

Mitchell, Charlie. "Black Hat founder sees software liability as major cybersecurity policy challenge." *Inside Cybersecurity*. July 26, 2017. https://insidecybersecurity.com/daily-news/black-hat-founder-sees-software-liability-major-cybersecurity-policy-challenge.

National Highway Traffic Safety Administration (NHTSA). "Cybersecurity Best Practices for Modern Vehicles." October 2016. https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

NIAC. "Securing Cyber Assets—Addressing Urgent Cyber Threats to Critical Infrastructure." August 2017. https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf.

Network Functions Virtualization—White Paper on NFV Priorities for 5G. February 21, 2017. https://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf.

NICCS. NICE Cybersecurity Workforce Framework. https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.

NICCS. "Cybersecurity Workforce Development Toolkit—How to Build a Strong Cybersecurity Workforce." March 2017. https://niccs.us-cert.gov/sites/default/files/documents/pdf/cybersecurity_workforce_development_toolkit.pdf?trackDocs=cybersecurity_workforce_development_toolkit.pdf.

National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity*. February 12, 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

NIST. Special Publication 800-193. *Platform Firmware Resiliency Guidelines.* May 2017. https://csrc.nist.gov/csrc/media/publications/sp/800-193/draft/documents/sp800-193-draft.pdf

NIST Information Technology Laboratory (ITL) Bulletin. *Dramatically Reducing Software Vulnerabilities.* January 2017. http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=922589.

NIST ITL Bulletin. *Tailoring Security Controls for Industrial Control Systems.* November 2015. http://csrc.nist.gov/publications/nistbul/itlbul2015_11.pdf.

National Telecommunications and Information Administration (NTIA). *Catalog of Existing IoT Security Standards (Draft Version 0.01),* NTIA Multistakeholder Process on IoT Security Upgradability and Patching, Existing Standards, Tools, and Initiatives Working Group. July 2017. https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog.pdf.

NTIA. Communications Sector Coordinating Council. *Industry Technical White Paper*. July 17, 2017. https://www.ntia.doc.gov/files/ntia/publications/cscc_industrywhitepaper_cover_letter.pdf.

NTIA. *Multistakeholder Process: Cybersecurity Vulnerabilities.* December 15, 2016. https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

NSTAC. *NSTAC Report to the President on the Internet of Things*. November 19, 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

O'Hern, Bill. AT&T, Inc. *Briefing to the NSTAC ICR Subcommittee*. July 20, 2017.

Olmstead, Kenneth and Aaron Smith. "Americans and Cybersecurity." *Pew Research Center Report.* at 19. January 26, 2017. http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf.

Pahl, Thomas B. FTC. *Start with security – and stick with it*. July 28, 2017. https://www.ftc.gov/news-events/blogs/business-blog/2017/07/start-security-stick-it.

SafeCode. https://safecode.org/about-safecode/.

Samani, Raj. McAfee, UK. *Briefing to the NSTAC ICR Subcommittee*. August 15, 2017.

Sann, Wallace. ForeScout. *Briefing to the NSTAC ICR Subcommittee*. August 22, 2017.

Sandvine, *Global Internet Phenomena: Encrypted Internet Traffic*. 2016. https://www.sandvine.com/resources/global-internet-phenomena/spotlight/internet-traffic-encryption.html.

Schneier, Bruce. *We Need to Save the Internet from the Internet of Things*. October 6, 2016. https://www.schneier.com/essays/archives/2016/10/we_need_to_save_the_.html.

Scriffignano, Anthony. Dun & Bradstreet, Inc. *Briefing to the NSTAC ICR Subcommittee.* August 15, 2017.

Spamhaus Project. *The World's Worst Botnet Countries.* August 18, 2017. https://www.spamhaus.org/statistics/botnet-cc/.

Symantec. *Mirai: What you need to know about the botnet behind recent major DDoS attacks.* October 27, 2016. https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks.

Tooley, Matt. National Cable and Television Association (NCTA), Communications Sector Coordinating Council, *Industry Technical White Paper on Botnets and Automated Threats*.

U.S. Chamber Institute for Legal Reform. "Torts of the Future—Addressing the Liability and Regulatory Implications of Emerging Technologies." March 2017. http://www.instituteforlegalreform.com/uploads/sites/1/_Torts_of_the_Future_Addressing_the_Liability_and_Regulatory_Implications_of_Emerging_Technologies_April_2017.pdf?pagename=uploads/sites/1/Torts_of_the_Future_Addressing_the_Liability_and_Regulatory_Implications_of_Emerging_Technologies_.pdf.

Wallach, Steve. Micron Technology, Inc. *Briefing to the NSTAC ICR Subcommittee*. September 7, 2017.

Walsh, Kevin. Palo Alto Networks, Inc. *Briefing to the NSTAC ICR Subcommittee*. July 18, 2017.

Warner, Mark. "Senators Introduce Bipartisan Legislation to Improve Cybersecurity of Internet of Things Devices." *Press Release*. August 1, 2017. https://www.warner.senate.gov/public/index.cfm/pressreleases?ID=06A5E941-FBC3-4A63-B9B4-523E18DADB36.

White House Office of the Press Secretary. *Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. May 11, 2017. https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

Xfinity. *Comcast List of Blocked Ports*. https://www.xfinity.com/support/internet/list-of-blocked-ports/.

Zetter, Kim. "Hacker Lexicon: What are DoS and DDoS Attacks?" *Wired.* January 16, 2016. https://www.wired.com/2016/01/hacker-lexicon-what-are-dos-and-ddos-attacks/.