A Report to the President

on

Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats

Transmitted by
The Secretary of Commerce
and
The Secretary of Homeland Security

DRAFT FOR PUBLIC COMMENT
January 5, 2018

Table of Contents

Executive Summary

This draft report responds to the May 11, 2017, Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. That order called for "resilience against botnets and other automated, distributed threats," directing the Secretary of Commerce, together with the Secretary of Homeland Security, to "lead an open and transparent process to identify and promote action by appropriate stakeholders" with the goal of "dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)."

The Departments of Commerce and Homeland Security worked jointly on this effort through three approaches—hosting a workshop, publishing a request for comment, and initiating an inquiry through the President's National Security Telecommunications Advisory Committee (NSTAC)—aimed at gathering a broad range of input from experts and stakeholders, including private industry, academia, and civil society. These activities contributed to the information gathering process for the agencies developing the recommendations in this draft report. The draft will be finalized based on adjudication of received comments before submission to the President. The final report is due to the President on May 11, 2018.

The Departments worked in consultation with the Departments of Defense, Justice, and State, the Federal Bureau of Investigation, the sector-specific agencies, the Federal Communications Commission and Federal Trade Commission, and other interested agencies.

The Departments determined that the opportunities and challenges in working toward dramatically reducing threats from automated, distributed attacks can be summarized in six principal themes.

1. **Automated, distributed attacks are a global problem.** The majority of the compromised devices in recent botnets have been geographically located outside the United States. Increasing the resilience of the Internet and communications ecosystem against these threats will require coordinated action with international partners.
2. **Effective tools exist, but are not widely used.** The tools, processes, and practices required to significantly enhance the resilience of the Internet and communications ecosystem are widely available, if imperfect, and are routinely applied in selected market sectors. However, they are not part of common practices for product development and deployment in many other sectors for a variety of reasons, including (but not limited to) lack of awareness, cost avoidance, insufficient technical expertise, and lack of market incentives.
3. **Products should be secured during all stages of the lifecycle.** Devices that are vulnerable at time of deployment, lack facilities to patch vulnerabilities after discovery, or remain in service after vendor support ends make assembling automated, distributed threats far too easy.
4. **Education and awareness is needed.** Knowledge gaps in home and enterprise customers, product developers, manufacturers, and infrastructure operators impede the deployment of the tools, processes, and practices that would make the ecosystem more resilient.
5. **Market incentives are misaligned.** Perceived market incentives do not align with the goal of "dramatically reducing threats perpetrated by automated and distributed attacks." Market incentives motivate product developers, manufacturers, and vendors to minimize cost and time to market, rather than to build in security or offer efficient security updates. There has to be a better balance between security and convenience when developing products.
6. **Automated, distributed attacks are an ecosystem-wide challenge.** No single stakeholder community can address the problem in isolation.

The Departments identified five complementary and mutually supportive goals that would dramatically reduce the threat of automated, distributed attacks and improve the resilience of the ecosystem. A list of suggested actions for key stakeholders reinforces each goal. The goals are:

- Goal 1: Identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace
- Goal 2: Promote innovation in the infrastructure for dynamic adaptation to evolving threats
- Goal 3: Promote innovation at the edge of the network to prevent, detect, and mitigate bad behavior
- Goal 4: Build coalitions between the security, infrastructure, and operational technology communities domestically and around the world
- Goal 5: Increase awareness and education across the ecosystem

The recommended actions and options include ongoing activities that should be continued or expanded, as well as new initiatives. No single investment or activity can mitigate all harms, but organized discussions and stakeholder feedback will allow us to further evaluate and prioritize these activities based on their expected return on investment and ability to measurably impact ecosystem resilience. As we release this draft report for public comment, we look to stakeholders to help us refine the value, utility, and investment potential of the proposed activities, the opportunities for support and leadership, and impediments to implementation.

I. Background

On May 11, 2017, the President issued Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," calling for "resilience against botnets and other automated, distributed threats."[1] The President directed the Secretary of Commerce and the Secretary of Homeland Security to "lead an open and transparent process to identify and promote action by appropriate stakeholders" with the goal of "dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)."

These types of attacks have been a concern since the early days of the Internet,[2] and were a regular occurrence by the early 2000s.[3] Automated and distributed attacks form a threat that reaches beyond any single company or sector. These threats are used for a variety of malicious activities, including distributed denial of service (DDoS) attacks that overwhelm networked resources, ransomware attacks that hold systems and data hostage, and computational propaganda campaigns[4] to manipulate and intimidate communities through social media. Traditional DDoS mitigation techniques, such as network providers building in excess capacity to absorb the effects of botnets, are designed to protect against botnets of an anticipated size. With new botnets that capitalize on the sheer number of "Internet of Things" (IoT) devices, DDoS attacks have grown in size to more than one terabit per second, outstripping expectations. As a result, recovery time from these types of attacks may be too slow, particularly when mission-critical services are involved. Further, these techniques were not designed to mitigate other classes of malicious activities, such as ransomware or computational propaganda.

As new scenarios emerge, there is an urgent need for coordination and collaboration across a diverse set of stakeholders. The federal government has worked with stakeholders in the past to address new threats as they arise. Previous efforts include the Industry Botnet Group, which led to the Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace (2012);[5] the Communications Security, Reliability and Interoperability Council's (CSRIC)[6] Anti-Bot Code of Conduct (2013),[7] and reports on

[1] Exec. Order No. 13,800, 82 Fed. Reg. 22,391 (May 11, 2017), *available at* https://www.federalregister.gov/d/2017-10004.

[2] United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

[3] *See, e.g.,* Nicholas C. Weaver, *Warhol Worms: The Potential for Very Fast Internet Plagues*, (2001), *available at* https://www1.icsi.berkeley.edu/~nweaver/papers/warhol/warhol.html.

[4] Computational propaganda is the assemblage of social media platforms, autonomous agents, and big data tasked with the manipulation of public opinion. Howard, PN and Woolley, SC, (2016), *Political communication, computational propaganda, and autonomous agents—Introduction*, International Journal of Communication, 10 (2016), 4882–4890, *available at* http://ijoc.org/index.php/ijoc/article/viewFile/6298/1809.

[5] Industry Botnet Group, *Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace*, https://archive.is/20131015084520/www.industrybotnetgroup.org/principles/.

[6] CSRIC is an advisory committee of the Federal Communications Commission, the mission of which is to make recommendations to the Commission to promote the security, reliability and resilience of the nation's communications systems. For more information, including past security efforts, *see* CSRIC, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0 (last visited December 6, 2017).

[7] Communications Security, Reliability and Interoperability Council III Working Group 7, *Final Report on U.S. Anti-Bot Code of Conduct (ABC) for Internet Services Providers (ISPs)*, (Mar. 2013), *available at* https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf.

Internet Service Provider (ISP) Network Protection Practices (2010)[8] and Remediation of Server-Based DDoS Attacks (2014);[9] and the active and ongoing work by the Department of Justice and its many partners on addressing and "sink-holing" the infrastructure supporting these threats.[10] While these initiatives have made some progress, the impacts have been incremental and significant challenges remain. By proactively addressing these challenges, this Administration and key stakeholders have an opportunity to enhance the resilience of the future Internet and communications ecosystem.

The DDoS attacks launched from the Mirai botnet in the fall of 2016, for example, reached a level of sustained traffic that overwhelmed many common DDoS mitigation tools and services, and even disrupted a Domain Name System (DNS) service that was a commonly used component in many DDoS mitigation strategies.[11] This attack also highlighted the growing insecurities in—and threats from—consumer-grade IoT devices. As a new technology, IoT devices are often built and deployed without important security features and practices in place.[12] While the original Mirai variant was relatively simple, exploiting weak device passwords, more sophisticated botnets have followed; for example, the Reaper botnet uses known code vulnerabilities to exploit a long list of devices.[13] The Mirai and Reaper botnets clearly demonstrate the risks posed by botnets of this size and scope, as well as the expected innovation and increased scale and complexity of future attacks.

Approach

The Departments of Commerce and Homeland Security worked jointly on this effort through three approaches aimed at gathering a broad range of input from experts and stakeholders, including private industry, academia, and civil society. The Departments worked in consultation with the Departments of Defense, Justice, and State, the Federal Bureau of Investigation, the sector-specific agencies, the Federal Communications Commission, and Federal Trade Commission, as well as other interested agencies.

In June 2017, Commerce's National Telecommunications and Information Administration (NTIA) issued a Request for Comment (RFC) on "Promoting Stakeholder Action Against Botnets and Other Automated Threats."[14] The RFC asked for feedback on "current, emerging, and potential approaches for dealing with

[8] Communications Security, Reliability and Interoperability Council Working Group 8, *Final Report on Internet Service Provider (ISP) Network Protection Practices*, (Dec. 2010), *available at* http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf.

[9] Communications Security, Reliability and Interoperability Council IV Working Group 5, *Final Report on Remediation of Server-Based DDoS Attacks*, (Sept. 2014), *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG5_Remediation_of_Server-Based_DDoS_Attacks_Report_Final_(pdf)_V11.pdf.

[10] *See, e.g.*, U.S. Department of Justice, *Avalanche Network Dismantled in International Cyber Operation*, (Dec. 5, 2016), https://www.justice.gov/opa/pr/avalanche-network-dismantled-international-cyber-operation.

[11] United States Computer Emergency Readiness Team, *Alert (TA16-288A): Heightened DDoS Threat Posed by Mirai and Other Botnets*, https://www.us-cert.gov/ncas/alerts/TA16-288A (last revised Oct. 17, 2017).

[12] The National Security Telecommunications Advisory Committee, *NSTAC Report to the President on the Internet of Things*, (Nov. 2014), *available at* 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.

[13] Brian Krebs, *Fear the Reaper, or Reaper Madness?*, Krebs on Security (Oct. 27, 2017), https://krebsonsecurity.com/2017/10/fear-the-reaper-or-reaper-madness/.

[14] Additional information, including the public comments, is available at National Telecommunications and Information Administration, *Request for Comments on Promoting Stakeholder Action Against Botnets and Other*

botnets and other distributed, automated attacks." NTIA received 47 comments, with respondents ranging from large trade associations to individual technical experts. The commenters also represented a diverse range of industries and sectors, including Internet service providers, security firms, infrastructure providers, software manufacturers, civil society, and academia.

In July 2017, Commerce's National Institute of Standards and Technology (NIST) hosted a workshop on "Enhancing Resilience of the Internet and Communications Ecosystem."[15] The workshop was designed to allow stakeholders to explore current and emerging solutions addressing automated, distributed threats in an open and transparent manner. It attracted 150 participants from diverse stakeholder communities, who identified a broad range of coordinated actions by all stakeholders to address these threats.

The Department of Homeland Security's (DHS) participation in this effort was focused through the President's National Security Telecommunications Advisory Committee's (NSTAC) Internet and Communications Resilience subcommittee, which finalized and approved the *NSTAC Report to the President on Internet and Communications Resilience* on November 16, 2017.[16] While developing its report, the NSTAC studied botnets, as well as forms of attacks that may be facilitated by botnets, such as DDoS attacks and vectors that could be used to create botnets (i.e., end user devices and IoT). Through its study, the NSTAC concluded that automated and distributed attacks facilitated through botnets threaten the security and resilience of the Internet and communications ecosystem, and in turn, the nation's critical infrastructure. Additionally, the NSTAC determined that compromised IoT devices will increasingly be used by malicious actors to launch global automated attacks.

These activities contributed to the information-gathering process for agencies developing the recommendations in this draft report. This draft is being posted for a 30-day public comment period. The draft will be finalized based on adjudication of received comments before submission to the President. The final report is due to the President on May 11, 2018.

Principal Themes

The opportunities and challenges we face in working toward dramatically reducing threats from automated, distributed attacks can be summarized in six principal themes.

1. **Automated, distributed attacks are a global problem.** The majority of the compromised devices in recent botnets have been geographically located outside the United States. Increasing the resilience of the Internet and communications ecosystem against these threats will require coordinated action with international partners.

Automated Threats, (June 8, 2017), https://www.ntia.doc.gov/federal-register-notice/2017/rfc-promoting-stakeholder-action-against-botnets-and-other-automated-threats.

[15] National Institute of Standards and Technology, *Enhancing Resilience of the Internet and Communications Ecosystem*, https://www.nist.gov/news-events/events/2017/07/enhancing-resilience-internet-and-communications-ecosystem (last updated July 10, 2017). For a summary of the proceedings, *see* Tim Polk, *Enhancing Resilience of the Internet and Communications Ecosystem: A NIST Workshop Proceedings* (Sept. 2017), NIST Interagency/Internal Report No. 8192, *available at* http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8192.pdf.

[16] The National Security Telecommunications Advisory Committee, *NSTAC Report to the President on Internet and Communications Resilience*, (2017), *available at* https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20DRAFT%20-%20508%20compliant.pdf.

2. **Effective tools exist, but are not widely used.** The tools, processes, and practices required to significantly enhance the resilience of the Internet and communications ecosystem are widely available, if imperfect, and are routinely applied in selected market sectors. However, they are not part of common practices for product development and deployment in many other sectors for a variety of reasons, including (but not limited to) lack of awareness, cost avoidance, insufficient technical expertise, and lack of market incentives.
3. **Products should be secured during all stages of the lifecycle.** Devices that are vulnerable at time of deployment, lack facilities to patch vulnerabilities after discovery, or remain in service after vendor support ends make assembling automated, distributed threats far too easy.
4. **Education and awareness is needed.** Knowledge gaps in home and enterprise customers, product developers, manufacturers, and infrastructure operators impede the deployment of the tools, processes, and practices that would make the ecosystem more resilient. In particular, customer-friendly mechanisms to identify more secure choices analogous to the Energy Star program[17] or National Highway Traffic Safety Administration (NHTSA) 5- Star Safety Ratings[18] are needed to inform buying decisions.
5. **Market incentives are misaligned.** Perceived market incentives do not align with the goal of "dramatically reducing threats perpetrated by automated and distributed attacks." Market incentives motivate product developers, manufacturers, and vendors to minimize cost and time to market, rather than to build in security or offer efficient security updates. There has to be a better balance between security and convenience when developing products.
6. **Automated, distributed attacks are an ecosystem-wide challenge.** No single stakeholder community can address the problem in isolation.

A Note About Threats

This paper does not differentiate between nation-states, cyber-criminals, and other threat actors. While some attacks may be difficult to initially attribute, the ecosystem still must come together to mitigate an attack. This open and transparent process focused on areas that would elicit the widest participation from stakeholders across the Internet and communications ecosystem regarding security improvements, as well as regarding cooperation before, during, and after attacks, understanding that the identity of a given threat actor may be initially unknown. The 2017 Worldwide Threat Assessment of the U.S. Intelligence Community released by the Office of the Director of National Intelligence provides insight into the cyber threat landscape.[19]

II. Current Status of the Ecosystem and Vision for the Future

This section describes the current status of the technical and policy domains of the Internet and communications ecosystem, and envisions an improved future. (Section III proposes a set of goals and

[17] Energy Star, *About Energy Star*, https://www.energystar.gov/about (last visited December 6, 2017).
[18] National Highway Traffic Safety Administration, *Search NHTSA's 5-Star Safety Ratings,* https://www.safercar.gov/Vehicle-Shoppers (last visited December 6, 2017).
[19] *See* Daniel R. Coats, Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Committee*, Statement for the Record at the Senate Select Committee on Intelligence (May 11, 2017), *available at* https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf.

supporting actions to work toward that future.) The technical domains identify the information and communication technology that compose the ecosystem. The technical domains of the ecosystem include:

- The ***infrastructure*** that connects the other technical domains into a single system;
- ***Enterprise networks*** composed of locally connected devices with Regional Internet Registry (RIR)[20]-assigned Internet Protocol (IP) version 4 (IPv4) and IPv6 Internet addresses;
- ***Edge devices*** such as servers, personal computers, mobile devices, and other connected devices; and
- ***Home and small business networks*** composed of devices using "private address space" addressable externally through network address translation (NAT).

The policy domain is intertwined with the technical domains, and includes:

- **Public-private partnerships**, including information-sharing arrangements;
- **Voluntary attestation or certification processes**, where vendors and customers opt-in to shared security goals and expectations;
- **Standards and guidelines** developed in multistakeholder fora;
- **Procurement policies**, especially within the federal government, to create market incentives;
- **Regulatory and legislative actions** at the federal and/or state levels; and
- **Multi- and bi-lateral coordination/agreements** to institutionalize international coordination and collaboration, including Internet governance.

Improved resilience against automated, distributed attacks will require coordination on policy and governance solutions across nations, sectors, and technical layers. Effective policies will provide clear expectations for use of standards and best practices while remaining flexible as the security risk evolves. Better information sharing across the domains will improve the ability of ecosystem members to mitigate the botnet threat. Meanwhile, some coordination models may require the creation of new standards, guidelines, and metrics.

Technical Domains

Infrastructure

In the face of automated, distributed attacks, the current infrastructure underlying the digital ecosystem has demonstrated remarkable resilience, but the increasing size and scope of attacks appear to be testing the limits of that resilience. These two perspectives arose after the 2016 Mirai botnet attacks that temporarily interrupted services of an Internet infrastructure provider, disrupting many major online services and websites in North America and Europe. However, the disruptions were temporary, and key players responded quickly. This response underscores both the interdependence of the infrastructure, and the ability of individuals and organizations to quickly learn and adapt.

In this report, "infrastructure" includes the technology and organizations that enable connectivity, interoperability, and stability, going beyond the physical wires, wireless transmitters and receivers, and satellite links to include the hardware, software, tools, standards, and practices on which the ecosystem

[20] "Regional Internet Registries are nonprofit corporations that administer and register Internet Protocol (IP) address space and Autonomous System (AS) numbers within a defined region." American Registry for Internet Numbers, *Regional Internet Registries*, https://www.arin.net/knowledge/rirs.html (last visited December 6, 2017).

depends—for example, routers, switches, Internet service providers, DNS providers, content delivery networks, hosting and cloud-service providers.[21] Because of the complexity of modern infrastructure, with key tools and players interspersed through the ecosystem, no single tool can secure the infrastructure. Traditionally, as new threats emerge, particular subsets of infrastructure players work together to understand the risk and the path to mitigation. No single framework is globally applicable, although many infrastructure participants have begun to use risk management tools.[22]

Filtering traffic as it enters and exits a network—a technique known as ingress and egress filtering—is one such tool. IP-spoofing is a common technique employed in DDoS attacks, where the attacker fabricates the source IP address to prevent the victim from filtering bad traffic by its origin. Network providers can limit spoofing by restricting incoming traffic to that which is actually originating from its stated network, filtering out traffic that claims to come from outside its expected network space.[23] Ingress filtering is acknowledged to be a longstanding best practice by the Internet Engineering Task Force (IETF) and other infrastructure-focused organizations.[24] It can be complemented by egress filtering, in which an organization or network operator deploys filters at the edge of its network to prevent traffic that does not appear to originate from inside the network from exiting onto the global Internet.

Major domestic carriers implement the ingress filtering standards in at least some portion of their network. However, these standards are not universally supported worldwide, or by smaller domestic ISPs. Many technical and business experts have objected to proposals to apply ingress filtering higher up in the Internet, at the level of international backbones. Egress filtering is advocated as a common security practice for enterprises,[25] but is still uncommon for small and medium-sized enterprises. Although not universally implemented, network ingress/egress filtering, where implemented, is effective at mitigating the class of DDoS attacks that leverage IP-source address spoofing.

Infrastructure providers and other companies offer commercial anti-DDoS services, which can play a key role in limiting the impacts of attacks against particular targets. However, not all enterprise customers purchase the full slate of anti-DDoS services, due to the expense and the complexity of integrating those services into the other components of the enterprise's network. Meanwhile, attackers quickly learn to exploit holes in existing services. When confronted by attacks that rely on the sheer volume of traffic, off-premise DDoS mitigation solutions either provision more network capacity or use the shape of the network itself to limit the volume of traffic that reaches the target. Other attacks target the web server

[21] While HSPD-7 recognizes the systems and assets of the telecommunications and information technology sectors as critical infrastructure, this document uses the term "Internet infrastructure" to additionally encompass the organizations and practices upon which the Internet ecosystem depends.

[22] Communications Security, Reliability and Interoperability Council IV Working Group 4, *Final Report on Cybersecurity Risk Management and Best Practices*, (Mar. 2015), *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[23] DHS is developing and supporting open-source software tools to assess and report on the deployment of source address validation (SAV) best anti-spoofing practices. For more information, *see* Center for Applied Internet Data Analysis, *Spoofer*, https://www.caida.org/projects/spoofer/ (last modified Dec. 8, 2017).

[24] *See, e.g.*, P. Ferguson & D. Senie, *Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing*, (May 2000), Internet Engineering Task Force – Network Working Group, *available at* https://tools.ietf.org/html/bcp38 ("BCP 38"); and F. Baker & P. Savola, *Ingress Filtering for Multihomed Networks*, (Mar. 2004), Internet Engineering Task Force – Network Working Group, *available at* https://tools.ietf.org/html/bcp84 ("BCP 84").

[25] *See, e.g.*, Chris Brenton, *Egress Filtering FAQ*, SANS Institute, https://www.sans.org/reading-room/whitepapers/firewalls/egress-filtering-faq-1059 (last revised Apr. 19, 2006).

or application itself. Enterprises' on-premise devices and tools detect and filter these attacks on the target network.

The current best practices involve employing a hybrid approach that uses both local filtering and off-premise capacity-increasing DDoS defense tools. However, best practices are at times expensive, difficult to manage, and require skilled staff; they are also typically built around past crises, making it difficult to argue for a large amount of excess capacity, for example, until under attack. An active threat detection program that detects vulnerabilities and attack trends can supplement these efforts, and the victim organization can respond as needed. Content delivery networks (CDNs) are another tool that can leverage large, dedicated private infrastructures to protect customers. As different attacks emerge, or adversaries select new targets, organizations often invest in threat-specific defenses.

Responding in a timely fashion requires preparation and knowledge. Given the large set of security controls needed in the modern Internet, not all staff at smaller ISPs or key enterprises are aware of the benefits of filtering and other tools. Many ISPs offer warnings about compromises and ongoing attacks, but if enterprises ignore those notices and warnings, then the ISP is less likely to diligently follow up with further notifications. Victims often struggle when encountering their first substantial attack without a response plan in place, because they depend on the very network under attack to understand it and contact service providers for aid.

Vision for the Future of Infrastructure

Infrastructure providers across the board must develop a broad understanding of the benefits of shared defense approaches, and communities should work together to drive best practice adoption. This work includes ubiquitous adoption of filtering at the interface with customer networks, including multi-tenant infrastructures such as cloud providers. Ideally, infrastructure providers should understand the current levels of attacks, maintain sufficient capacity to absorb realistically expected levels of malicious traffic, and communicate those capabilities to their customers. Infrastructure-provider services for DDoS mitigation should integrate with customers' existing network solutions, regardless of the level of service a customer has chosen. An increasingly smart network can segment different types of traffic automatically, to isolate or mitigate applications or devices that are sources of attacks. Enterprises are increasingly able to address application-level attacks with appropriate tools, and the vendors of these tools should work with both customers and the relevant application vendors to make security decisions easier and more efficient. As new products and tools become available, players across the ecosystem should understand how their behavior can help—or hinder—their efficacy.

Increased implementation of a number of existing technologies will help mitigate these attacks. Some of the existing infrastructure is built on older protocols, such as the IPv4 network and legacy routing protocols. Broader adoption of current standards and best practices will bring security benefits. For example, the IPv6 network can better enable device-specific recognition across the network to detect device-level aberrant behavior.[26] Small and mid-sized organizations should incorporate industry best practices, and, as new infrastructure standards and practices are needed and proven, infrastructure providers should efficiently adopt them.

[26] It is important to note, however, that the current IPv4 workaround, Network Address Translation (NAT), does offer real firewalling benefits, especially at the home network level. Security experts have also expressed concern about the security of some IPv6 implementations.

At the core of the infrastructure, key players already share information about the evolving nature of threats. While many of these organizations employ experts who coordinate with their peers around the globe, in the future, information sharing must extend to smaller, less well-funded, or niche players through new automated tools and practices. Incentives could promote investment in better, more efficient detection of malicious traffic, as well as more public commitments to avoid carrying malicious traffic. These commitments would build on existing relationships across the community to help build a more stable global network.

Enterprise Networks

Networks that support enterprises (e.g., medium and large businesses, government agencies, and academic institutions) are another key technical domain in the Internet and communications ecosystem. These networks are often complex, with enterprise-owned and -operated Border Gateway Protocol (BGP) routers, DNS resolvers, and applications that rely on a mix of local and cloud-based services. Edge devices often include powerful servers, personal computing devices, mobile phones, and managed and unmanaged IoT devices. Devices on enterprise networks can use a mixture of statically or dynamically assigned addresses from one or more public IP address ranges (e.g., addresses acquired from an RIR) as well as addresses assigned from locally administered private IP address ranges.

The large presence of enterprise networks connected to the Internet means that they are simultaneously a victim and source of risk. Automated, distributed threats present significant risks to enterprises and their operations. Many well-known DDoS attacks, such as the attacks on U.S. banks in 2012 and 2013, targeted customer-facing services associated with large enterprises.[27] Enterprises in the U.S. and overseas have been victimized by ransomware attacks, including hospitals in the U.S. and UK.[28]

Resources associated with enterprise networks have also been a significant factor in executing automated, distributed threats. Devices at enterprises, ranging from IoT devices to data center servers, have been compromised and incorporated into botnets. Poorly administered enterprise resources, such as open DNS resolvers, are often leveraged to amplify attacks. Enterprise-operated routers that do not enforce ingress and egress filtering have facilitated attacks that featured address spoofing, allowing botnet participants to hide their true locations. In the special case of cloud providers, enterprise resources have been rented (usually with stolen credit cards) to quickly assemble significant botnets.

Enterprises that have faced DDoS attacks in the past, or that are from sectors broadly impacted by these attacks, often build potential attacks into their risk model and employ a mix of DDoS mitigations offered by infrastructure providers and enterprise managed on-premise mitigations. Enterprises that understand the risks and implement these mechanisms are the exception. Many at-risk enterprises are unaware of the potential impacts of DDoS attacks on their operations. Such enterprises may not understand fully their ability to protect their networks and respond to an attack. For example, they may not understand the limitations of their contracts with Internet service providers, or the availability of products and services to mitigate DDoS attacks. They also may not understand fully the cost to recover from such an attack.

[27] *See* David Goldman, *Major Banks Hit With Biggest Cyberattacks in History*, CNN (Sept. 28, 2012, 9:27 AM ET), http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html.

[28] *See* Russell Brandom, *UK Hospitals Hit With Massive Ransomware Attack*, The Verge (May 12, 2017, 11:36 AM EDT), https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin.

In the absence of an ongoing attack, enterprises traditionally focus on availability, functionality, and cost. As a result, enterprises will rely on legacy devices that can no longer be adequately secured, or will deploy IoT and other devices that were never designed to be secure. Where devices are eligible for security updates, enterprises may have extremely onerous processes to evaluate patches or long periods between scheduled maintenance, expanding the window of vulnerability.[29]

While enterprises typically have professional information technology (IT) operations staff, cybersecurity-specific expertise is often lacking. This challenge is often compounded by a similar lack of awareness among organizations' decision makers, who are responsible for resourcing IT operations within their organizations or for overseeing the IT operations. IT operations teams are often unaware of the risks of open resolvers and other sources of attack amplification, or the importance of ingress and egress filtering. When ISPs report potential compromise to customers, they often find that the enterprise cannot identify or locate the compromised devices, and even if the enterprise can identify the devices, it may not have the tools or expertise to recover to a secure state. Enterprises may struggle to work collaboratively with service providers when under attack. Failure to implement basic backup procedures places enterprises at greater risk from ransomware attacks.

Enterprises can contribute to a more resilient ecosystem through a mix of current and emerging technologies, operational and procurement policies, and education and awareness for IT staff and decision makers.

A Vision for the Future of Enterprise Networks

A foundational step toward this vision would be widespread enterprise application of the NIST Cybersecurity Framework (CSF).[30] Most of the necessary actions can be ascribed to the five concurrent and continuous functions:

- **Identify.** Enterprises locate legacy devices and other devices that cannot be secured. Enterprises remove these high-risk devices from service wherever possible and replace them with devices that are inherently secure or can be secured.
- **Protect.** The system architecture provides additional layers of protection to any remaining high-risk devices (e.g., access to legacy devices would be restricted by network architecture). Enterprises deploy or procure on- and off-premise DDoS mitigation services. Enterprises' network architectures limit exposure of devices to malicious actors and limit damage from compromised devices. Ingress and egress filtering are implemented to prevent network address spoofing, and attack amplifiers (e.g., open resolvers) are reconfigured. Efficient update processes minimize the window of vulnerability for all devices on the network. Multi-tenant infrastructures also enforce ingress and egress filtering to reduce the impact of cloud-based botnets.
- **Detect.** A combination of ISP-based detection services and enterprise-operated network and service monitoring detect outbound malicious traffic, inbound attacks, and identify compromised devices in near real-time.
- **Respond.** Enterprises have policies and procedures to address compromised devices when detected (by the enterprise or ISP). Enterprises also have processes in place to contact their

[29] *See* Dan Goodin, *Failure to Patch Two-month-old Bug Led to Massive Equifax Breach*, Ars Technica (Sept. 13, 2017, 11:12 PM), https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/.

[30] National Institute of Standards and Technology, *Cybersecurity Framework*, https://www.nist.gov/cybersecurity-framework (last visited December 6, 2017).

ISP(s) or other anti-DDoS service providers when attacks are detected locally. Key operational resources continue to operate with constrained resources.

- **Recover.** Enterprises have the ability to reconstitute compromised systems (e.g., from backup) rather than submit ransomware payments to resume operations.

The technologies and operational policies highlighted above are realistic only if supported by an appropriate mix of education and awareness initiatives and procurement policies. Enterprise staff and management must be aware of security risks to enterprise resources from distributed threats, and options for mitigation and prevention. IT staff must possess the skills to implement the selected options for mitigation and prevention. Organizational procurement policies must ensure that security lifecycle issues figure prominently in procurement decisions, so insecure products are not added to the mix.

Last, but not least, these changes must occur in enterprises globally, rather than just domestically, to have significant impact on the ecosystem. In many countries, the issues surrounding legacy systems are compounded by the widespread use of pirated software. Such enterprises are nearly impossible to protect, providing malicious actors with a reservoir of easily compromised systems to assemble into distributed threats.

Edge Devices

Devices are a diverse and growing technical domain of the ecosystem. The Internet simultaneously supports multi-user computing systems, personal computing and mobile devices, and operational technology (e.g., supervisory control and data acquisition [SCADA] in industrial/manufacturing settings), and IoT in homes and offices. As a general rule, edge devices play two diametrically opposed roles with respect to distributed threats: malicious actors compromise edge devices to create distributed threats, and edge devices may also be the target of the threat (e.g., ransomware attacks). Poorly secured endpoints can be both the source and victim of attacks.

Malicious actors are motivated to construct botnets as cheaply and efficiently as possible. Over the years, the target of choice has evolved from multi-user systems to personal computers, then to cloud services (using stolen credit cards), and more recently to IoT devices. These shifts in targeting reflect the promise and challenges offered by this technical domain with respect to creating a more resilient ecosystem. Personal computers and mobile devices are more secure than in years past. Meanwhile, connected devices have reached a level of sophistication and density that facilitates their targeting by automated code, while the benefits of modern security tools are lacking in those devices.

Edge devices may be vulnerable to compromise for a variety of reasons:

- Often, devices were not designed with security in mind. Developers are either unaware of good security design practices, assume that the device will be inaccessible (e.g., on a local network air gapped from the Internet), or want to avoid security solutions that impose additional cost or increase time to market. The resulting design choices, such as hard-coded administrative passwords, create inherently insecure devices. In other cases, appropriate security controls are present but usability/user interfaces result in less-secure configurations.

- Common software development techniques result in, optimistically, a flaw every 2,000 lines of code[31]—or more by many other metrics.[32] Many of these bugs create exploitable security vulnerabilities, such as buffer overflows.
- When bugs are discovered after products are deployed, products may be difficult or impossible to patch. These vulnerabilities are often far easier to exploit than to correct.
- Systems shipped with inappropriate default configuration settings, such as hard-coded passwords, are more vulnerable in operation.
- Systems may also be vulnerable because support is unavailable. This is often the case for old devices.

A number of major software developers have taken these lessons to heart and have established best current practices that can significantly reduce vulnerabilities of edge devices. For example, Microsoft's Software Development Life Cycle, or SDLC, ensures that security is considered from the beginning. Secure software development tools, such as input fuzzing or static analysis, reduce the number of vulnerabilities in software. Secure update services can correct vulnerabilities after discovery.[33] Systems are shipped in more secure configurations, so default settings need not be changed. As a result, modern servers, desktops, laptops, and smart phones offer significantly fewer opportunities for compromise, and this translates to the cloud environment as well, demonstrating that more-secure edge devices are a now a practical possibility. Hardware roots of trust, demonstrating that systems have not been tampered with, are another innovation appearing in modern systems.

Unfortunately, the state of the art for IoT devices is much like that of desktop computing in the 1990s. Vendors developing operating systems and applications for traditional computing devices have gained experience with secure configuration defaults, security patching regimens, and tools for central management. IoT devices are often sorely lacking in such security-focused features. These systems now offer the most attractive target to malicious actors, and are an increasingly large percentage of the devices in the ecosystem. In fact, the November 2016 Ericsson Mobility Report predicted that IoT devices will surpass mobile phones as the largest category of connected devices in 2018.[34] Given the level of security on these devices, that is a daunting prediction.

In addition, this domain of the ecosystem is not composed solely of modern devices. There are many legacy servers, desktops, laptops, and mobile phones in use today, and this will be the case for the foreseeable future. Legacy devices are no longer supported by their manufacturer, so their

[31] *See Coverity Scan: Open Source Report 2014*, Synopsys, page 4 (2015), http://go.coverity.com/rs/157-LQW-289/images/2014-Coverity-Scan-Report.pdf.

[32] *See, e.g.,* Steve McConnell, *Code Complete: A Practical Handbook of Software Construction*, pages 521, 652, (Microsoft Press, 2nd ed. 2004), ISBN: 0735619670.

[33] The Software Assurance Forum for Excellence in Code (SAFECode), an industry consortium, has released a report to codify these lessons and offer further guidance on the SDLC model. Mark Belk et al., *Fundamental Practices for Secure Software Development 2nd Edition: A Guide to the Most Effective Secure Development Practices in Use Today*, SAFECode, (Feb. 8, 2011), *available at* https://www.safecode.org/wp-content/uploads/2014/09/SAFECode_Dev_Practices0211.pdf.

[34] Ericsson, *Ericsson Mobility Report: On the Pulse of the Networked Society*, (Nov. 2016), https://www.ericsson.com/assets/local/mobility-report/documents/2016/ericsson-mobility-report-november-2016.pdf.

vulnerabilities cannot be easily addressed.[35] To make matters worse, attack tools for these devices or their vulnerable code components were often developed long ago and remain widely available.

Finally, high percentages of personal computing systems on the Internet run pirated software; one industry association's statistics for 2015 ranged from 17% in the U.S. to 70% in China and 84% in Indonesia.[36] Manufacturers typically restrict the distribution of security patches only to systems running legally purchased software, so these systems cannot be secured against known vulnerabilities. While vendors cannot reasonably be expected to provide support for unlicensed software, these unprotected systems provide another class of easy targets for malicious actors.

Insecure devices are not a result of limitations in the underlying technology. Applied properly, the current best practices are fairly effective, if imperfect, and result in devices that are reasonably secure upon delivery, and include tools to maintain that level of security throughout the device's lifecycle. Commercial sectors that have embraced these practices, such as operating system developers, have demonstrated significant improvements in security and resilience.[37] Unfortunately, these security practices are implemented inconsistently. Many products are shipped with known bugs, do not include an update mechanism, and/or do not follow best current practices for administrative access.

Some of this challenge is an education and awareness problem. Product developers do not understand how to leverage currently available tools for secure product development. Operational technology product developers understand their product line (e.g., refrigerators) but do not understand basic security requirements for their products' network connectivity. Enterprise customers make procurement decisions without considering full lifecycle costs, as well as externalities of having an insecure network. End consumers may lack the tools to understand how certain product features protect them from security risks.

Perceived market incentives exacerbate the problem.[38] Product developers prioritize time-to-market and innovative functionality over security and resilience. Security features are not easily understood or communicated to the consumer, which makes it difficult to generate demand.

Vision for the Future of Edge Devices

Broad advances in the Edge Device technical domain are both possible and essential if we are to build a more resilient Internet and communications ecosystem. To be effective, these advances must be global, since the majority of Internet devices are located outside the United States. This global action will require globally accepted security standards and practices to be robust, widely understood, and applied ubiquitously. Those standards should be flexible, appropriately timed, open, voluntary, industry-driven, and global in nature.

[35] For example, Microsoft discontinued support for twelve-year old Windows XP in April 2014. Two years later, between 7.4 and 10.9% of the PCs on the Internet were still running XP and were described as "sitting ducks for cybercriminals to attack." John Zorabedian, *Millions of People Are Still Running Windows XP*, Naked Security (Apr. 11, 2016), https://nakedsecurity.sophos.com/2016/04/11/millions-of-people-are-still-running-windows-xp/.

[36] *See* BSA | The Software Alliance, *Seizing Opportunity Through License Compliance: BSA Global Software Survey*, (May 2016), http://www.bsa.org/~/media/Files/StudiesDownload/BSA_GSS_US.pdf.

[37] *See* Steven J. Vaughan-Nichols, *Security 2014: The Holes Are in the Apps, not the Operating Systems*, ZDNet (Feb. 28, 2014, 19:46 GMT), http://www.zdnet.com/article/security-2014-the-holes-are-in-the-apps-not-the-operating-systems/.

[38] The ISOC report on security in routing suggests some consumers would pay a premium for better security.

Devices must be able to resist attacks throughout their deployment lifecycles—at the time of shipment, during use, and through to end-of-life. For this to occur, security must become a primary design goal. Vendors must not ship products with known serious security flaws, must include a secure update mechanism, and must follow best current practices (e.g., no hard-coded passwords, disabling software features that are not critical to operation) for system configuration and administration. The expected period of use and duration of support must be clearly communicated to customers, and device manufacturers should maintain secure update services for the promised duration.

Hardware roots of trust and trusted execution technologies are now a component of many off-the-shelf computing platforms. Future products will need to leverage these technologies to demonstrate authenticity and integrity at initial deployment and throughout the period of use. Modern development techniques rely on a combination of open source and commercially available components. To meet future security demands, such components must be traceable through the supply chain and offer greater assurance.

Such advances will require significant steps forward in education and awareness for product developers. All product developers must be equipped with the knowledge and skills required to apply the available tools for secure product development. The tool kits and components used by these vendors must reflect security concerns to achieve scale and keep pace with a changing developer workforce, and the partnerships and consortia driving standardized technology must empower developers to make and communicate security decisions. Operational-technology product developers must add basic security requirements to their product specific knowledge and skills. Customers must be equipped with sufficient knowledge and information to select products designed to be secure in their environment, and aware of the risks presented by legacy devices.

Lastly, the market incentives will need to align with these security advances, so that product developers who prioritize security and resilience equally with time-to-market and innovative functionality are rewarded with increased market share. Clear signals regarding product security and resilience that are accessible to customers will help improve these incentives. However, the value proposition for better security will likely start in the enterprise environment; once there is a generally accepted security posture in a given product class, few manufacturers would be likely to ignore it.

Home and Small Business Networks

Home and small business networks are becoming increasingly complex. Traditional computing devices on premises interact with the cloud and other service providers to support an ever-increasing array of business and personal applications. IoT devices are already proliferating in great numbers in consumers' homes, from home automation devices such as lights, garage door openers, and thermostats, to connected home appliances and personal health and fitness monitors. This is the case in small businesses as well, where entrepreneurs and managers may seek to gain the benefit of off-the-shelf technology but lack an administrator or concerted IT strategies or policies. By all estimations, the number of connected consumer devices is expected to grow. Unfortunately, this area of growth is also an area in which security is seriously lacking. The vast majority of home and small business users are unaware of cybersecurity risks, and many do not take the most basic security measures when connecting devices to their networks. Security-relevant decisions may be reached without customer input or knowledge if the IoT device is set up and configured by someone else on their behalf or if the device uses a network other than the consumer's own network (for example, a cell network).

As in the areas detailed above, many tools generally exist to mitigate cybersecurity risk, but the general population is unlikely to be able to navigate the complex security environment. Home network products are not typically designed in a way that would allow home users to easily segment networks or configure security policies. Many home users rely on legacy devices or unlicensed systems. Furthermore, when a home user's device does become part of a botnet, it is often difficult for the network provider to tell which device is transmitting; the NAT function, which allows home users to share a single IPv4 address among numerous devices behind a home router, also obscures which device is being exploited.[39]

In the home and small business market, most home devices are unmanaged and thus unlikely to be updated manually, if automatic update features are not available. Consumer devices often ship with outdated software containing known vulnerabilities or hard-coded administrative passwords. Typical users may not be able to determine if the device's software is up to date or if it even has a mechanism for software updates—many consumer devices do not. The typical user may not even be aware of the importance of this aspect, and is unlikely to have access to substantive information about the software on a given device at all.

Generally, home and small business users do not have easy access to the information they need to select secure products and they typically do not have tools to manage the products they have. While enterprise gateways are more likely to provide integrated security offerings, home users are unlikely to have access to the same level of service, and for those who do, many are not aware of the security offerings or the reason those services should be implemented. Fundamental security steps, such as changing a device's password when you add the device to your network, are often beyond consumers' awareness or capabilities. In some instances, poor implementation of such requirements can frustrate users' efforts to implement basic practices such as changing default passwords or enabling secure encryption.

Some device manufacturers have expressed concern that consumers will not pay more for devices with better security. The reality is that consumers are not directly affected by compromises of their devices; in fact, the consumer may never know that the device is part of a botnet. From the consumer's perspective, the webcam is still streaming, or the refrigerator is still chilling. For this reason, it is impractical to hold the owners responsible if their devices are used in a botnet. This lack of clear consequences of infection creates a challenge in motivating consumers to take steps to improve security, for example, to update even those devices that are updateable.

Vision of the Future for Home and Small Business Networks

It is unrealistic to expect home users and small business proprietors to become security experts. Instead of assuming these consumers will change their behavior, a more effective tack is to engineer devices with users' behavior in mind. Ideally, devices marketed toward consumers should be designed with security built in. Consumer products should be designed as securely as possible, should include secure automated update mechanisms, and should have few to no requirements for managing the products.

Ideally, consumers will have access to commercial offerings that implement best current security practices, and will be able to easily recognize those offerings. Small business owners will similarly be able to map their purchases to their unique security concerns and obligations. They will be aware of the

[39] We also note that NAT technology offers some security benefits by limiting inbound traffic access to specific endpoints. This impedes (but does not completely eliminate) the threat from automated scanning and infection tools.

various risks related to unsecure IoT devices, and they will choose devices that are more secure. Nonprofits and commercial entities have begun evaluating products for privacy and data security;[40] efforts like this will raise awareness, and as awareness increases, so should device makers' interest in secure development. Over time, it should become easier and cheaper for manufacturers and integrators to adopt a secure development lifecycle.

While home users may not be especially motivated by fear that their devices could be used in a botnet, they may feel more compelled by concerns that their privacy, data, or access to services could be compromised. Since many connected devices use cloud services for management, this can further highlight the importance of security and privacy needs. Fortunately, many of the same security steps they would take to improve their privacy or data security and ensure uninterrupted access to services would also mitigate the chance of their devices becoming part of a botnet.

Market forces will also play a key role in improved device security. For widely used consumer devices to become more secure overall, better security should not cost significantly more than insecure devices. Consumer products and services should be engineered with basic privacy and security protections built in. Buying guides that are easy to comprehend and provide actionable recommendations, targeted at specific home and small business needs, can generate the necessary market signals to reward developers and vendors for investing in security.

Smart routers and firewalls should be widely used to mitigate attacks and detect when a device has been compromised. As more home users' IoT devices transition to publicly addressable IPv6 addresses, ISPs will find it easier to identify end devices transmitting malicious traffic. Home users' networks enforce virtual network segmentation. Limiting devices' capabilities based on their intended uses—for example, limiting a connected toaster's activities on the network to solely those activities required to perform its toasting duties—would significantly limit the ability of botnets to capture home devices. A global decline in the home use of legacy products and pirated software would also vastly limit botnet perpetrators' opportunities.

Home users should be able to identify devices on their networks that increase their cybersecurity risk. Research and development is occurring to help security-conscious consumers better manage their networks. In 2017, the Federal Trade Commission's (FTC) IoT Home Inspector Challenge awarded its top prize for a proposal for a mobile app-based tool that would help users manage the IoT devices in their homes. The app would flag devices with out-of-date software and other common vulnerabilities and provide instructions on how to update each device's software and fix other vulnerabilities.

Consumer education will need to become more effective, even if devices are better engineered to consumers' expected skill level. Meanwhile, there is an opportunity for a new workforce to support consumers' and small businesses' networking needs; this role could become a new vocation, more akin to electricians than electrical engineers, with appropriate training. The network and device industries can also make support easier and cheaper through standardization and coordination.

[40] Consumer Reports, *Consumer Reports to Begin Evaluating Products, Services for Privacy and Data Security*, (Mar. 6, 2017), *available at* https://www.consumerreports.org/privacy/consumer-reports-to-begin-evaluating-products-services-for-privacy-and-data-security/.

Governance, Policy, and Coordination

Because automated, distributed attacks on the global Internet are an ecosystem-wide problem, the issue will require coordination on policy and governance solutions across sectors. No single actor or sector is responsible for single-handedly addressing these risks, and no single entity can simply say that these risks are all someone else's problem. For example, while many solutions involve active coordination with ISPs, putting sole responsibility at the network level would make all traffic dependent on this connective layer to determine what "good" traffic looks like, empowering ISPs to decide what fundamentally is and is not allowed on the Internet. Moreover, such ISP decision making would invariably both block traffic that in fact is "good," and miss traffic that should be blocked.

Given the networked nature of the risks, real coordination is necessary to fully understand the problem and identify paths to solutions. While the information technology and communications sectors do actively work to understand security risks, sectors often are unable to coordinate well with other sectors. Even though some entities coordinate domestically or regionally, there are few global mechanisms to share information about threats, solutions, and their adoption and efficacy. In many cases, lack of clarity around roles and responsibilities has impeded collective action, resulting in security failures.

Keeping in mind that this problem is global in nature, international cooperation must be emphasized. Some governments have a poor track record when it comes to governance in dynamic sectors; regulations that are overly specific quickly become obsolete and can hinder innovation and limit consumer/user benefit. Compliance requirements, or mandating specific regulations, may address some risks, but often carry with them a greater burden while still leaving the broader ecosystem insecure. The regulatory picture is further complicated by state or local regulation of edge devices, operational technology, and infrastructure. Solutions specific to particular countries or jurisdictions put at risk the global nature of an ecosystem where both bits and products flow with relative ease.

This problem is further compounded by the cross-domain nature of networked technology. Lines have blurred between consumer technology, enterprise-grade tools and devices on which organizations depend, and safety-critical technology on which lives can depend. The same hardware and software can be used across the entire ecosystem. Key infrastructure services can be used by both a video game network and a company's corporate network.

In the law enforcement area, industry cooperation in taking down botnets is improving, but is not yet commonplace. Recent successful botnet takedowns involved extensive collaboration with industry: for example, Kelihos, Gameover Zeus, and Coreflood. Active collaboration between law enforcement and private actors like Microsoft has enabled disruption through private seizures of key command and control assets. A new rule in 2016 has helped facilitate the work involved in botnet takedowns; Federal Rule of Criminal Procedure 41(b)(6) was amended to address the unique challenges in investigating botnet activity, clarifying that courts may issues search warrants authorizing the search of multiple computers when the identified computers are located in multiple judicial districts. However, taking down botnets in a safe, secure manner is a labor-intensive and lengthy process, and is complicated by the need to cooperate across jurisdictions to identify and prosecute malicious actors. In addition, federal law enforcement's ability to obtain civil injunctions—which has been indispensable in past botnet takedowns—is limited to cases that include elements of wiretapping or certain types of fraud.

Vision for the Future of Governance, Policy, and Coordination

In the future, purchasers, whether end consumers or sophisticated enterprises, should be better able to understand the basic security properties of connected devices. Approaches to IoT and computing devices are needed that will help not only promote consumer awareness, but will also drive the market, increasing the general adoption and use of better cybersecurity practices by device makers. That said, security risk evolves quickly; that which is deemed secure today may not be secure tomorrow, and is unlikely to be secure a decade from now. Market transparency solutions can empower buyers to make good decisions, but must also build in the context and timescale of the product lifecycle. Institutions that have relied on approaches that traditionally reflected static risk, such as purchasing requirements or insurance, will adapt to reflect the evolving nature of cybersecurity risk. Improved transparency about the software and hardware components of systems will help, as will appropriate incentives to understand the relevant risks for a given context.

Infrastructure players will better share and analyze data to foster a shared awareness of reputations across the ecosystem, and evaluate how well network partners are addressing risks in an evolving, efficient, decentralized manner. Mechanisms for information sharing would ideally build on existing multistakeholder mechanisms and communities, and would create new opportunities to engage locally and globally.

As distributed threats evolve, new standards, guidelines, and metrics may be required to answer new and emerging questions such as: How can third-parties best evaluate products for consumer benefits in a manner that is agile enough to keep up with quickly evolving security practices? What metrics and visibility into network management practice can inform us about infrastructure investment? More formalized and adaptable security expectations will allow us to introduce some accountability into security practices. Governance mechanisms, such as shared norms or frameworks, can help shape incentives to require good design and create some accountability for failure to consider security and invest in secure devices. Any accountability mechanisms should reward those who make good risk-based decisions, while acknowledging that there is no such thing as perfect security.

More broadly, to address the range of threats, inter-sector, interagency, and international action must improve to more fully address automated, distributed attacks. At its core, that involves reducing the number of unsecured devices with access to the Internet to keep botnets to a manageable size, and developing mechanisms to share information about compromised systems and emerging attack trends up and down the stack to the party that is in the best position to respond to the threat.

Because technology deployment is truly trans-national and data flow across international borders, none of this can be accomplished without international coordination. In the international realm, the U.S. government robustly advocates for industry-led approaches and consensus-based standards. As the NSTAC report stated, solutions depend on both standards and innovation at the network and Internet infrastructure layer. While a variety of standards and best practices exist, they are not adopted consistently across the globe.

Both the U.S. government and international partners should conduct their technology and device procurement actions to create market incentives for more secure products, while recognizing the advantages of open, voluntary, industry-driven standards. Engagement should grow between the anti-abuse and global network infrastructure communities, as well as between cybersecurity and operational technology elements of industries that have not traditionally been technically focused (e.g., critical infrastructure or medical devices) communities. International coordination will be key around the Internet resources used by botnet managers for command and control. The U.S. should increase its international engagement, particularly with countries that are already active on this issue.

From a law enforcement perspective, industry and law enforcement should work to find ways to coordinate more often and earlier to detect and prevent threat activity, and in managing incidents that take place. New tools and processes may improve information sharing among international law enforcement agencies. Law enforcement and industry groups should more effectively communicate on what is needed to successfully disrupt malicious networks and prosecute the actors behind it, while listening in turn to the concerns of the privacy community. Additionally, law enforcement and industry should coordinate closely to ensure emerging technologies, including IoT devices, meet cybersecurity standards to prevent the further spread of botnets to such technologies. Data-protection policies, both in the U.S. and internationally, should not disrupt existing tools, such as the widely used WHOIS database of domain ownership data.

Legal Landscape

Some stakeholders stressed the importance of minimizing uncertainty and legal risk to encourage private-sector collaboration with law enforcement agencies, more information sharing, vulnerability disclosure, and the ability to conduct effective countermeasures. Many also emphasized the need to harmonize legal approaches across sectors to avoid a patchwork of laws that could impede the IoT market.

Efforts are already underway to improve public-private relationships. DHS's National Cybersecurity and Communications Integration Center (NCCIC) serves as a central location where a diverse set of private sector and government partners involved in cybersecurity coordinate and synchronize their efforts,[41] including information sharing, collaboration, and technical assistance.[42] Federal law also already includes a structure for addressing some of the uncertainty and legal risk. The Cybersecurity Information Sharing Act of 2015 (CISA), for example, grants liability protection and other legal protections—such as antitrust protections, exceptions from disclosure laws and certain regulatory uses, and protections from privilege waivers, to private entities that share cyber threat indicators and defensive measures in compliance with the act.[43] CISA designates the NCCIC as a central hub for the sharing of cyber threat indicators and defensive measures with the federal government.[44] These NCCIC cybersecurity capabilities and CISA legal protections apply to IoT cybersecurity in much the same way that they apply to cybersecurity more broadly. Moreover, nothing in CISA precludes robust sharing by private entities with law enforcement as part of the normal course of a criminal investigation; indeed, CISA authorizes the sharing of cyber threat indicators and defensive measures

[41] *See* 6 U.S.C. § 148.

[42] *Id.* § 148(c).

[43] *See* Consolidated Appropriations Act, 2016, Division N – Cybersecurity Act of 2015 (Pub. L. No. 114-113, 129 Stat. 2242) (codified at 6 U.S.C. §§ 1501-1510).

[44] CISA provides an array of legal protections for cyber threat indicators and defensive measures that are shared with a federal entity in accordance with the statute. For instance, it provides protection from antitrust liability (6 U.S.C. § 1503(e)); federal and state disclosure laws (6 U.S.C. §§ 1503(d)(3) and (d)(4)(B)); waiver of privileges (6 U.S.C. § 1504(d)(1)); and federal and state regulatory use (6 U.S.C. §§ 1503(d)(4)(C) and 1504 (d)(5)(D)). When cyber threat indicators and defensive measures are shared with the NCCIC through the Federal government's capability and process operated by DHS, such sharing also receives additional liability protections. 6 U.S.C. § 1504(c)(1)(B). Those additional liability protections are also available for sharing with other federal entities under limited circumstances. *See* 6 U.S.C. § 1504(c)(1)(B)(i) and (ii).

with law enforcement—or any other federal entity—and, in addition, its liability protection applies when such information is shared with law enforcement under certain circumstances.

Many stakeholders also stressed the importance of market incentives for securing IoT devices. Some touched on whether a liability regime informed by common best practices and standards might improve accountability in IoT device security. While this report does not engage in a comprehensive analysis of liability related to IoT device security, we expect this issue will continue to garner interest as the use of connected devices—devices that can impact the physical world—grows and questions regarding harms, causal chains, risk management, and possible state and court actions emerge. Liability is a complex area of law, as is the emerging IoT market, and care must be taken to avoid static and ineffectual compliance requirements, especially in the midst of a dynamic cybersecurity landscape. Investment must be made to address risk through innovative practices, and with stakeholders engaged in cross-sector coordination. Pressure to directly address this issue will grow if legal uncertainty is endemic and persistent.

III. Goals and Actions

These goals and actions aim to present a comprehensive portfolio of mutually supportive actions and options that, if implemented, would improve the resilience of the ecosystem. The recommended actions and options include ongoing activities that should be continued or expanded, as well as new initiatives. No single investment or activity can mitigate all harms, but organized discussions and stakeholder feedback will allow us to further evaluate and prioritize these activities based on their expected return on investment and ability to measurably impact ecosystem resilience. As we release this draft report for public comment, we look to stakeholders to help us refine the value, utility, and investment potential of the proposed activities, the opportunities for support and leadership, and impediments to implementation.

Goal 1: Identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace

To enhance the resilience of the Internet and communications ecosystem, it is critical that our technology marketplace support and reward the continuous development, adoption, and evolution of innovative security technologies and processes. When market incentives encourage manufacturers to feature security innovations as a balanced complement to functionality and performance, adoption of tools and processes that result in highly secure products is easier to justify. As these tools become more popular, increased demand will drive further research. As such tools are refined, it becomes cheaper for manufacturers and integrators to adopt the components of a secure development lifecycle, encouraging more manufacturers to compete on security. This section identifies actions that key stakeholders can take to establish an adaptable, sustainable, and secure technology marketplace.

Action 1.1 Establish broadly accepted baseline security profiles for IoT devices in home and industrial applications, and promote international adoption through bilateral arrangements and the use of international standards. The federal government should accelerate this process by adopting baseline security profiles for IoT devices in U.S. government environments.

Security standards, profiles, and best practices have evolved over time for traditional computing devices, increasing the cost of assembling botnets with these devices. Rapidly increasing deployment of insecure IoT devices has the pernicious side effect of enabling cost-effective development of extremely large and widely distributed botnets. The vulnerability of new IOT devices is not a flaw inherent to the technology; the best current security practices for traditional computing devices include well-known and effective countermeasures with straightforward application to IoT. For example, best current security practices require secure default configuration and effective software update mechanisms. The Mirai botnets have compromised hundreds of thousands of devices as a result of hard-coded administrative passwords; although reports vary on its size—some reporting upwards of a million devices primed for malicious use—the Reaper botnet has compromised devices by targeting well-known software vulnerabilities. While mitigations exist, many of the affected devices are not patchable.

The impact of past botnets has been mitigated by actions taken by ISPs—mainly absorbing excess traffic and cease and desist actions—but past mitigations were mainly reactive by nature, and the increase in IoT devices indicates diminishing returns for these traditional mitigation strategies. The ecosystem must become more resilient to distributed threats, starting with reducing the known vulnerability of Internet-connected devices throughout the lifecycle. Objective baseline security profiles appropriate for home and industrial applications of IoT are needed to accelerate the development and deployment of IoT devices that are less vulnerable to compromise. Security profiles identify suites of complementary standards and security mechanisms that represent the combination of current best practices appropriate for a particular threat environment. Customer-supported profiles appropriate for home and industrial applications would provide a signal to the market that the customers will prefer IoT devices that meet the baseline. The profiles would also provide an immediate opportunity for product differentiation and a basis for future assessment programs (See Action 5.1). The NIST National Cybersecurity Center of Excellence has produced a number of such profiles for IoT, healthcare devices, manufacturing, and other types of devices and target industries.[45]

The federal government should augment the existing suite of standards and practices for traditional computing with baseline security profiles for IoT devices in U.S. government environments. By developing federal IoT security profiles in coordination with industry and international partners, the federal government can establish the practicality and efficacy of profiles and create a starting point for more general efforts. The U.S. government and industry should also jointly engage with developers of international standards and specifications, such as the IETF and the Joint Technical Committee 1 of the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (ISO/IEC-JTC1), to establish globally relevant standards. As these standards evolve, federal profiles should be re-aligned or replaced as appropriate.

Standards and specifications should be developed in private-sector bodies that are open to participation by all interested stakeholders, and should be developed in a transparent manner, using consensus-based processes; such standards and specifications are well suited for addressing the challenges posed by a rapidly evolving technology space. These processes do not exclude government participation, but ensure that government, industry, and users' interests are all well represented and the resulting solutions reflect the state of art in that technology space. The flexibility of these processes also enables standards to be updated as technology, threats, and solutions evolve. The strong alignment between businesses' use of standards that they helped develop and governments' participation in the

[45] *See* National Institute of Standards and Technology, National Cybersecurity Center of Excellence, *Projects*, https://nccoe.nist.gov/projects (last visited December 6, 2017).

development of these tools facilitates adoption of these standards on a large scale. It is important to recognize that, given the breadth of the technology space, no single standards or specification development organization can develop all the solutions. Governments around the world need to support cooperation and coordination between standards and specification bodies that have the expertise and experience and develop products along the principles discussed earlier in this paragraph, to ensure robust, timely, and fit-for-purpose solutions. NIST should lead and coordinate federal agencies' engagement on related standards activities, including engagement with the private sector, exploring a federal government strategy for international standards to address the challenges of botnets and other automated, distributed threats.

Complementary actions by the U.S. government and private sector could significantly enhance the impacts of these profiles. The federal government can use acquisition rules and procurement guidelines to amplify the market signal by requiring certain security features or properties (see Action 2.3). The private sector could establish an assessment and labeling mechanism for products that comply with the home profile (see Action 5.1). The private sector could also work with existing programs or establish new programs to evaluate products that comply with the industrial profile (see Action 5.2).

Action 1.2 Software development tools and processes to significantly reduce the incidence of security vulnerabilities in commercial-off-the-shelf software must be more widely adopted by industry. The federal government should collaborate with industry to encourage further enhancement and application of these practices and to improve marketplace adoption and accountability.

Common software development techniques result in software with at least one bug per 2,000 lines of code,[46] and modern systems include tens of millions of lines of code. This implies tens of thousands of bugs in a system, and many of these bugs create security vulnerabilities. The secure update mechanisms noted in Action 1.1 allow vendors to correct these errors after a relatively brief vulnerability period. However, avoiding such vulnerabilities altogether would have an even more significant impact. In fact, it is possible to develop code with very small numbers of errors, where the importance of the mission merits the reduction in productivity. The challenge is developing mechanisms that produce significantly better code without unduly reducing productivity.

An interagency task force (documented in NISTIR 8151[47]) identified numerous approaches to developing software with fewer vulnerabilities, implementing three basic strategies:

- Stopping vulnerabilities before they occur, including improved methods for specifying and building software;
- Finding vulnerabilities, including better testing techniques and more efficient use of multiple testing methods; and
- Reducing the impact of vulnerabilities by building architectures that are more resilient, so that vulnerabilities cannot be meaningfully exploited.

[46] *See Coverity Scan: Open Source Report 2014*, Synopsys, page 4, (2015), http://go.coverity.com/rs/157-LQW-289/images/2014-Coverity-Scan-Report.pdf.

[47] Paul E. Black, Lee Badger, Barbara Guttman & Elizabeth Fong, *Dramatically Reducing Software Vulnerabilities: Report to the White House Office of Science and Technology Policy*, (Nov. 2016), NIST Interagency/Internal Report No. 8151, *available at* http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8151.pdf.

Tools to support these approaches are available now,[48] and have been embraced by a few forward-leaning firms.[49] Software developers should begin transitioning to these tools immediately, focusing initially on the products that present the highest risk. DHS and the FTC offer resources for smaller software developers as well.[50]

The federal government should support industry adoption of these tools through efforts that improve return on investment or create market incentives for lagging sectors or industry groups, as the NSTAC also recommended. The federal government should promote the further development of tools for secure coding practices by sponsoring or performing targeted research (see Action 1.3), and sponsoring competitions for secure toolchains (multi-tool processes for software development) to demonstrate their effectiveness and productivity. The federal government should also work with industry to develop strategies that make it easier and cheaper to adopt these approaches, and work with the full range of stakeholders to make such a process observable and verifiable to third parties.

As an example, modern products use many software components, libraries, and modules, some of which may be outdated or vulnerable and are not always closely tracked by manufacturers in the rapid development cycle. NTIA should engage diverse stakeholders in examining the role of transparency tools and practices in improving manufacturers and purchasers understanding of what goes into IoT products, such as by documenting the off-the-shelf software and firmware included in a product or device. By bringing together developers and vendors with enterprise customers and vulnerability management solution providers, the community as a whole can leverage existing tools and practices to improve business processes and catalyze a more efficient market for secure products. If widely adopted, transparency tools and practices could generate market forces for better security, and allow assurances that no known vulnerabilities are shipped with products. Knowing what software has been incorporated into a product is a fundamental step toward being able to keep it updated and mitigate threats when they arise.

Action 1.3 Industry should expedite the development and deployment of innovative technologies for prevention and mitigation of distributed threats. Accordingly, where applicable, government should prioritize the application of research and development (R&D) funds and technology transition efforts to support advancement in DDoS prevention and mitigation, as well as foundational technologies to prevent botnet creation.

The rapid growth in DDoS capacity offered by IoT-based botnets imperils the effectiveness of current DDoS mitigation techniques. Research and development in techniques that offer mitigation closer to the source, or leverage machine learning/artificial intelligence (AI), is urgently needed to get ahead of malicious actors. New innovations will be needed to address other botnet-supported malicious

[48] *See, e.g.*, *CWE/SANS Top 25 Most Dangerous Software* Errors, SANS Institute, https://www.sans.org/top25-software-errors/ (last updated June 27, 2011).

[49] For example, the Software Assurance Marketplace (SWAMP) aims to make it easier to consistently test the quality and security of these applications and bring a transformative change to the software assurance landscape by reducing the number of weaknesses deployed in software. For more information, *see* Software Assurance Marketplace, https://continuousassurance.org/ (last visited December 6, 2017).

[50] DHS supported the development of the SWAMP, which offers both cloud-based and open source software assurance tools. For more information, *see* Software Assurance Marketplace, *About Swamp*, https://continuousassurance.org/about-us/ (last visited Dec. 20, 2017); Federal Trade Commission, *Careful Connections: Building Security in the Internet of Things*, (Jan. 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf.

activities, such as ransomware and computational propaganda. Foundational technologies to prevent, detect, and recover from compromise and incorporation into a botnet will be required to address these and future attacks.

To enhance the resilience of the ecosystem, successes in research and development must be capitalized upon through aggressive deployment. Innovative device technologies, such as hardware roots of trust or enhanced device authentication mechanisms, offer the potential for significantly stronger security throughout the product lifecycle. Advances in network tools, such as the Manufacturer's Usage Description (MUD), a standard currently under development in the IETF,[51] could enhance the resilience of the network by managing communications for security and making granular network management cheaper and easier. Accelerated adoption of such innovative technologies would positively impact the resilience of the ecosystem, but commercialization and adoption of promising research results to create viable products or marketable services is notoriously challenging.

The federal government should support this action through targeted funding and collaborative technology transition activities. The federal government is the primary source of funding for basic research in cybersecurity. Departments and agencies (D/As) also sponsor applied research in support of mission requirements and a variety of technology transition activities.[52] D/As should prioritize development and deployment of innovations that would increase the resilience of the ecosystem and coordinate these investments through the Networking and Information Technology Research and Development (NITRD) program.[53]

Action 1.4 Government and industry should collaborate to ensure existing best practices, frameworks, and guidelines relevant to IoT, as well as procedures to ensure transparency, are more widely adopted across the digital ecosystem.

Several previous efforts have produced guidance and best practices related to botnets and better IoT security, but botnets remain a problem. Publishing documents is not enough—they must be widely adopted across the ecosystem. For example, the stakeholders in NTIA's multistakeholder process on IoT Security Upgradability and Patching developed a set of documents offering solutions to both the supply and demand side of the IoT consumer market, but stakeholders also emphasized the shared role in promoting these ideas across the IoT community.[54] The IoT community must work collaboratively to identify and adopt existing best practices, frameworks, and guidelines that are relevant to IoT. The IoT community should also work to raise awareness of these best practices, frameworks, and guidelines.

[51] *See* E. Lear, R. Droms & D. Romascanu, *Manufacturer Usage Description Specification* (Draft), Internet Engineering Task Force – Network Working Group (Oct. 24, 2017), https://tools.ietf.org/html/draft-ietf-opsawg-mud-13.

[52] DHS's Distributed Denial of Service Defense project is an example of such research. *See* U.S. Department of Homeland Security, *Distributed Denial of Service Defense (DDoSD)*, https://www.dhs.gov/science-and-technology/csd-ddosd (last visited December 6, 2017). *See also* National Science Foundation, *Secure and Trustworthy Cyberspace (SaTC)*, https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709 (last visited December 6, 2017).

[53] The Networking and Information Technology Research and Development Program, https://www.nitrd.gov/ (last visited December 6, 2017).

[54] NTIA Multistakeholder Process on Internet of Things Upgradability and Patching. https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security (last updated November 7, 2017).

The NSTAC report also noted this need, related to its recommendation that industry should work with DHS and Commerce to accelerate adoption of security guidelines.

The federal government should support industry adoption of best practices by engaging the community to review prior activities and discuss reasons the prior recommendations were not widely implemented or were unsuccessful, identify appropriate paths for driving change in organizations, and focus on practical, proven tools and levers. For example, current development practices emphasize re-use of open source and commercial software, which may be outdated or vulnerable, but these attributes of (in)security are obscured from developers and customers alike. NTIA should engage stakeholders from both the vendor and enterprise customer communities to promote greater awareness and use of transparency tools and practices to allow both the supply side and the demand side to understand what goes into IoT products, generate market forces for better security through transparency, and increase assurances that no known vulnerabilities are shipped with products.

Complementary efforts to increase awareness and educate product developers and manufacturers could significantly enhance the impact of these best practices, frameworks, and guidelines, as described in Actions 5.3, 5.4, and 5.5.

Goal 2: Promote innovation in the infrastructure for dynamic adaptation to evolving threats

To establish a more resilient Internet and communications ecosystem, standards and practices that deter, prevent, and/or mitigate botnets and distributed threats should be continuously implemented and upgraded in all domains of the ecosystem in response to and anticipation of the evolving threat. This section identifies actions available to stakeholders to support development of an effective and dynamic infrastructure.

Action 2.1 Internet service providers and their peering partners should expand current information sharing to achieve more timely and effective sharing of actionable threat information both domestically and globally.

Once established, botnets are re-sold or rented to multiple customers and redirected to attack new targets in succession. This means many ISPs and their peering partners will experience similar attacks over time. When an ISP first faces a particular threat, anomalous behavior must be analyzed and mitigation methods developed. Bots are generally distributed across many ISPs, each of which can contribute to mitigation activities given sufficient knowledge. Sharing network management techniques and defensive tactics that are effective against particular threats is another way large network providers increase the preemptive value of the information shared.

By sharing information about known, ongoing, and emerging threats, ISPs may respond more efficiently. Current information-sharing arrangements are often driven by personal relationships and are not comprehensive. An evolving network landscape, and the changing scope, scale, focus and diversity of network players, also impacts the effectiveness of sharing relationships. Collaboration between ISPs and their peering partners should include sharing of detection, notification, and planned or utilized mitigation methods within the network. Where sharing is encumbered by commercial concerns, ISPs should seek ways to address sharing arrangements and response coordination in their peering and transit agreements.

Industry should lead efforts to expand the scope and utility of information sharing between ISPs and their peering partners and to address gaps in operationalizing the information shared. In particular, industry should work collaboratively with government to improve coordinated responses to actionable information and lead the development, refinement, and standardization of information sharing protocols to increase speed and permit automated response.

While industry has the lead role, the federal government can facilitate this activity domestically through the Communications Information Sharing and Analysis Center (ISAC) (i.e., the National Coordinating Center for Communications [NCC]), by forging partnerships with Network Operator Groups (NOGs), and internationally by expanding information-sharing agreements with international peers such as Telecom ISAC Japan. The government can play an important role in these discussions, convening multistakeholder discussions where needed, providing a global view, and ensuring that the process is equitable for all stakeholders.

Action 2.2 Stakeholders and subject matter experts, in consultation with NIST, should lead the development of a CSF Profile for Enterprise DDoS Prevention and Mitigation.

The Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) version 1.0 was developed by NIST with extensive private sector input. The CSF provides a flexible approach to managing cybersecurity risk that incorporates industry standards and best practices, is sufficiently general to allow for broad applicability in a variety of environments, and has been widely accepted by industry. The CSF may be supplemented by Framework Profiles, which apply the Framework components to a specific situation. In particular, profiles may be used by industry sectors to document best practices for protection against specific threats.

Through consultation with NIST, stakeholders including industry, academic and other subject matter experts should partner to develop a CSF Profile[55] for Enterprise DDoS Prevention and Mitigation, focusing on the desired state of organizational cybersecurity to mitigate DDoS attacks. The profile would help enterprises identify opportunities to improve DDoS threat mitigation and aid in cybersecurity prioritization by comparing their current state with the desired target state. The profile would likely include multiple levels to support industry sectors with different resilience requirements. Government stakeholders should participate in the development to ensure the profile is broadly applicable enough to contribute to a CSF Profile for Federal DDoS Prevention and Mitigation.

Action 2.3 The federal government should lead by example and demonstrate practicality of technologies, creating market incentives for early adopters.

Upon publication of the device IoT profiles (Action 1.1), the federal government should establish procurement guidelines to provide market incentives for early adopters. Many IoT product vendors have expressed desire to enhance the security of their products, but are concerned that market incentives are heavily weighted toward cost and time to market. Without evidence that customers will absorb the additional cost to develop more secure products, the industry continues a race to the bottom. While federal procurement no longer dominates the market, its buying power and influence is still strong, and the U.S. government can lead by example. By developing compliance guidelines for federal procurement actions based on the baseline security profiles for IoT devices, the U.S. government can establish market incentives for early adopters. The Office of Management and Budget, General Services Administration (GSA), and Department of Defense can facilitate these procurement requirements through policy and modifications to the GSA schedule and federal acquisition regulations.

[55] CSF Profiles are compilations of guidance and best practices around particular threats that follow the well-established CSF model.

Upon publication of an appropriate CSF profile (Action 2.2), the federal government should implement basic DDoS prevention and mitigation measures for all networks operated by or on behalf of departments and agencies to enhance the resilience of the ecosystem and demonstrate practicality and efficacy of the profile. In the past, federal networks have been implicated in DDoS attacks, where hackers have leveraged open resolvers and other agency resources to amplify their attacks. The federal Government should lead by example, ensuring that federal resources are not unwitting participants and that federal networks are prepared to detect, mitigate, and respond as necessary. The Administration should mandate implementation of the Federal CSF Profile for DDoS Prevention and Mitigation by all government agencies within a fixed period after completion and publication of the profile.

The federal government should evaluate and implement effective ways to mandate the use of software development tools and processes that significantly reduce the incidence of security vulnerabilities in all federal software procurements, such as through certification requirements. To establish market incentives for secure software development, the federal government should establish procurement regulations that favor or require commercial-off-the-shelf software developed using such processes, when available. The federal government should also ensure that internal software development projects use the best available tools to obtain insight into the impact of these regulations.

Action 2.4 Industry and government should collaborate with the full range of stakeholders to continue to enhance and standardize information-sharing protocols.

To address automated, distributed threats, stakeholders must share robust information in a timely (near real-time) manner. As a key lesson learned, the NSTAC report indicated that collaboration between the public and private sectors is vital to mitigating botnets. Information sharing protocols currently in use were pioneered by the federal government, with active input from a wide range of stakeholders. To meet the coordination and collaboration needs of a highly resilient infrastructure, these protocols must be comprehensive and sufficiently precise to permit automated processing and response. To ensure these goals are met, industry should lead efforts, in collaboration with the federal government and other stakeholders, to enhance information-sharing protocols to meet stakeholder needs and establish international standards to facilitate global coordination.

Action 2.5 The federal government should work with U.S. and global infrastructure providers to expand best practices on network traffic management across the ecosystem.

While network providers cannot be expected to serve as traffic cops and identify all bad packets, both common and newer tools and practices can help filter out some types of bad traffic. Many market actors use either informal reputation signaling or more formal peering and transit agreements to address traffic management. A broad coalition of experts—industry, academia, and government—should examine the extent to which inter-autonomous system (AS), internetwork peering, and transit agreements might improve traffic management accountability—for instance, as applied to anti-spoofing and filtering. The academic and engineering community should research how new tools and practices in development might also be incorporated and implemented. Industry and the federal government should build upon these findings to expand best practices on network traffic management across the ecosystem. Existing tools and frameworks, such as the U.S. Anti-Bot Code of Conduct for ISPs, should be reviewed, and new solutions should be explored in a multistakeholder process that includes a diverse representation of network players that map to today’s ecosystem environment.

Goal 3: Promote innovation at the edge of the network to prevent, detect, and mitigate bad behavior

To establish a resilient Internet and communications ecosystem, infrastructure services designed to protect against attacks should be complemented by increased detection and mitigation of compromised devices in home or enterprise networks, and where those networks connect to the Internet. More context from local knowledge can improve detection, and it may be easier to simply segment off or firewall particular devices or services behaving anomalously. This section identifies actions stakeholders can take to manage the impact of the compromised devices that comprise automated, distributed threats.

Action 3.1 The networking industry should expand current product development and standardization efforts for effective and secure traffic management in home and enterprise environments.

The networking industry is pursuing a variety of proprietary and standards-based mechanisms to better manage traffic within enterprise networks. These mechanisms aim to prevent communications with "suspicious" systems or constrain communications to hosts specifically required for correct operations. These systems may leverage AI/machine learning, information provided by external information sharing services, or device-specific information. Industry should expand these efforts to accelerate the delivery of efficient and cost-effective network security for both home and enterprise environments.

Local network hubs and gateways[56] can act as traffic managers, identifying and preventing malicious traffic from accessing IoT devices and limiting harmful traffic emanating from devices in the local network. Cloud providers are also developing solutions that might layer with these gateway-focused solutions, potentially providing multiple checks and balances in the network stack to better secure the IoT ecosystem. As these security innovations emerge, government and stakeholders should partner to increase awareness of security solutions among consumers, small and medium enterprises, and international partners. Where specific barriers to adoption or advancement exist, government and stakeholders should convene to identify obstacles, to amplify attention of the MUD standard, and to examine practical firewall policies for the broader product space.

Action 3.2 User interfaces on home IT and IoT products should be designed to maximize security while reducing or eliminating security knowledge requirements for administration.

Enterprise networks benefit from the attention of professional staff who are charged with maintaining the security of the network and systems. Such personnel are often aware of and sufficiently skilled to configure these devices to a secure baseline. The administrative interfaces for most IT and IoT devices are designed for personnel with this background and skill level.

The owners of home and small business networks are less likely to have such support, with the inevitable result of insecurely deployed networks and products. Rather than expect homeowners to become security experts, the IT and IoT industries should prioritize simple and straightforward deployment and configuration processes for devices marketed to home and small businesses. For example, if the installation process does not force updates to administrative passwords, these products will continue to be easy targets for incorporation into botnets. Default configurations should be the

[56] Gateways are network architecture components that sit between subcomponents of the network. *See supra* Section II for discussions around smart gateways, etc.

most secure for the intended scope of use, and cloud or application-based interfaces should be intuitive and rely on best current design practices.

Action 3.3 Enterprises should migrate to network architectures that facilitate detection, disruption, and mitigation of automated, distributed threats.

A variety of effective anti-DDoS products and services are currently available, and innovative new products (such as those described in Action 3.1) have recently emerged. However, most enterprises have architected their networks for simplicity and performance rather than security. In combination with the CSF Profile for DDoS Prevention and Mitigation, enterprises have an opportunity to re-architect their networks to isolate insecure devices, manage communication flows, and generally enhance the resilience of their corner of the ecosystem. For example, enterprises that depend upon legacy systems should architect their networks so that these insecure devices are not exposed to attacks from the general Internet. Some of this migration may occur organically as enterprises integrate more IoT devices into their networked environments; however, government, industry, and civil society should work to improve user and enterprise knowledge of threats and best security practices through collaborations such as partnership campaigns and strategic engagement activities.

Action 3.4 The federal government should investigate how wider IPv6 deployment can alter the economics of both attack and defense.

North America ran out of easily distributed unused IPv4 addresses in 2015, yet very few consumers and small businesses currently take advantage of IPv6 address space and capabilities. Government and industry have been planning and working for a broader IPv6 adoption, but should also consider how this will change the potential attack space and magnitude of automated, distributed attacks.

One challenge around notifying consumers that a device on their network has been linked to malicious activity is the large number of devices typically connected to a home or small business network. NAT-enabled routers, which can make many devices appear as if they have the same IP address, can impede notification. As we transition to IPv6, consumer ISPs may be better positioned to observe device-specific misbehavior when IPv6 addresses are not subjected to NAT. This information can, in turn, map to other edge-focused solutions.

Implementing NAT-enabled routers at the consumer and small business level has at times served as a key protection of vulnerable endpoints. NAT tools act as an incidental firewall, preventing devices in the home from being directly reached by the sort of mass-scanning tools that spread malware and lead to widespread infection; security cameras were a common target in the Mirai botnet because they typically do not sit behind a NAT-enabled router. In current architectures, a network that is IPv6-based would likely allow each device to be addressable. In theory, the IPv6 address space is so large that it would not be scannable using existing tools, but experts have observed that patterns would allow new scanning techniques to still discover vulnerable devices.

NTIA should work with stakeholders to identify lessons learned from industry and other countries, further examining impediments and options to align incentives to encourage ISPs to fully transition to IPv6 more quickly. Enabling the defense and mitigating the risk will require further innovation at the edge of the network. Understanding this sooner will provide for better solutions when IPv6 usage becomes more widespread.

Goal 4: Build coalitions between the security, infrastructure, and operational technology communities domestically and around the world

To enhance the resilience of the Internet and communications infrastructure, coordinated actions that cross geopolitical, public-private, industrial sector, and technical boundaries must become easier to implement. This section identifies key actions to increase engagement between critical stakeholder communities.

Action 4.1 ISPs and large enterprises should increase information sharing with law enforcement to provide more timely and actionable information regarding automated, distributed threats.

While many of the actions in this report will increase the cost or reduce the effectiveness of automated, distributed attacks, law enforcement actions have unique impacts on the botnet community. By taking down command and control systems, law enforcement can rapidly "lobotomize" a distributed threat. Prosecution of key players in the botnet economy not only slows the development of distributed threats by current participants, but also discourages prospective developers from joining in.

Law enforcement relies on ISPs and other key infrastructure providers to support ongoing investigations and other efforts to counter automated threats by providing actionable information about threats and trends affecting their networks and customers. By providing even more timely and actionable information, ISPs and other key infrastructure providers can facilitate, support, and accelerate law enforcement actions, including those that affect botnets distributed across the globe. Law enforcement can proactively lay out what kinds of data will help them investigate and prosecute bad actors, and work with infrastructure providers to make it cheaper and easier to share this information while protecting Internet user privacy. Government should perfect and streamline its approach to "sharing with one is sharing with all"[57] by ensuring that information received by law enforcement, where appropriate, is shared across the federal government through the cyber centers. With that said, law enforcement treats companies that have suffered an intrusion or distributed attack as victims of a crime, and conducts their investigations of such reported crimes with discretion to avoid the unwarranted release of information concerning the incident, whenever possible.

RIRs and registrars can facilitate attribution of bad actors by maintaining accurate WHOIS databases. In addition, the federal government should work to engage with its European counterparts to ensure that at least timely access to WHOIS information is preserved as the European data privacy protections are enforced to preserve a critical tool for domestic and global efforts to investigate botnets. Governments should work with private-sector entities responsible for compliance with data privacy protection regulations, as well as those entities involved in botnet investigatory work, to ensure that both equities are preserved (compliance and botnet investigations).

Action 4.2 The federal government should promote international adoption of best practices and relevant tools through bilateral and multilateral international engagement efforts.

Significant enhancements to the resilience of the ecosystem cannot be achieved through domestic action alone. The United States should lead engagement with international partners through regular bilateral and multilateral engagements on cybersecurity by leveraging expertise within the federal D/As. Where security issues relate to the security of the DNS, NTIA should lead coordination with federal

[57] This concept is not always applicable and may not resonate with some victims who are concerned about their confidentiality.

agencies and represent U.S. positions at multistakeholder fora, such as the Internet Corporation for Assigned Names and Numbers (ICANN).

International standardization could be particularly beneficial. Widely applicable international standards for IoT security could expand the market for products that contribute to the resilience of the ecosystem while leveling the playing field for American businesses. As the NSTAC report recommended, industry and federal agencies that participate in standards development should coordinate on a strategy for engaging within appropriate industry-driven international standards bodies to ensure U.S. representation and leadership, and through that participation, champion a flexible and interoperable suite of international standards for IoT security.

Action 4.3 Regulatory agencies should work with industry to ensure non-deceptive marketing and foster appropriate sector-specific security requirements.

Due to the complexity and diversity across the IoT landscape, it is difficult to envision a set of one-size-fits-all rules that could ensure security while keeping pace with the rate of change and the dynamic nature of the threat environment. Sector-specific regulatory agencies can, however, promote ecosystem resilience by working with industry to ensure products they regulate meet basic security requirements. For example, the Food and Drug Administration has established guidelines for medical devices that decouple basic security updates from existing product certification regimes.[58] These guidelines are beneficial to consumers, as the medical devices they rely on become more resilient against cybersecurity threats, and to manufacturers, who gain clarity regarding certification requirements. Stakeholders emphasized that the federal government might benefit from an interagency IoT coordination mechanism to promote and share these types of innovative practices and lessons learned, and to avoid regulatory conflicts.

Careful enforcement actions can benefit consumers and honest participants in the market. The FTC has taken action in numerous privacy and security-related cases, with IoT devices figuring in some of these enforcement actions.[59] By halting and deterring deceptive marketing, the FTC can enhance consumer confidence in security claims by IoT and information technology vendors and support positive market incentives. The FTC has also used its unfairness authority under Section 5 of the FTC Act to challenge unreasonable security practices, including in the IoT space. In addition, sector-specific agencies, such as U.S. Department of Health and Human Services, enforce information security regulations across the relevant industries. These policies can contribute to, and benefit from, the broader ecosystem security discussion.

Action 4.4 The community should take concrete steps to limit fast flux hosting.

"Fast flux hosting" is the automated, rapid modification of IP addresses assigned to hosts in the DNS to hide the location of websites supporting malicious, illegal, or criminal activities. A 2008 Security and Stability Advisory Committee (SSAC) Advisory[60] considered measures that certain registrars and registries implement today: monitoring changes to DNS records that are indicative of fast flux hosting, restricting DNS change frequencies and value ranges, and monitoring registrant account access to

[58] Food and Drug Administration, *Postmarket Management of Cybersecurity in Medical Devices*, (Dec. 28, 2016), *available at* https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

[59] *See, e.g.*, Federal Trade Commission, *In the Matter of TRENDnet, Inc.*, FTC Matter/File Number 122 3090, https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter (last updated Feb. 7, 2014).

[60] ICANN Security and Stability Advisory Committee, *SAC 025: SSAC Advisory on Fast Flux Hosting and DNS*, (Mar. 2008), https://www.icann.org/en/system/files/files/sac-025-en.pdf.

prevent automation. It further considered how registrars could apply such measures to expedite illegal website and domain name suspension processes. These measures could make a substantial difference in the efforts to curb botnet activity, but they haven't been widely implemented. New advances by attackers, including "double flux networks," require further innovation and collaboration at the network level. The broader community, including the federal government, should advocate within the relevant multistakeholder fora (e.g., ICANN and the RIRs) for wider implementation of these measures, or alternative mechanisms to achieve this objective.

Action 4.5 The cybersecurity community should continue to engage with the operational technology community to promote awareness and accelerate cybersecurity technology transfer.

The incorporation of networking functionality into operational technology has introduced new cybersecurity challenges that can be addressed only through the combined expertise of the cybersecurity and operational technology (OT) communities. The primary requirements associated with instances of OT are out of scope for cybersecurity subject matter experts, and OT subject matter experts are often unfamiliar with basic cybersecurity practices.

The federal government can facilitate this process by expanding current engagements that bring the cybersecurity and OT communities together to share knowledge and expertise and that promote awareness and accelerate technology transfer from the cybersecurity community. Sector-specific agencies work closely with their sectors to understand cyber risk, to link sectors to federal resources, and to promote resilience planning. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors and collaborates with international and private-sector Computer Incident Response Teams (CIRTs) to share control systems-related security incidents and mitigation measures. The federal government's cybersecurity community is currently pursuing device-specific engagements with specific OT communities, on topics such as secure updates for infusion pumps. The OT community should participate in the industry actions cited in this report to drive sector-specific solutions to their individualized cyber risks.

Goal 5: Increase awareness and education across the ecosystem

To enhance the resilience of the Internet and communications ecosystem against distributed threats, all stakeholders must recognize and be prepared to execute their roles and responsibilities. This section identifies actions that would close gaps between current skills and responsibilities.

Action 5.1 The private sector should establish and administer voluntary informational tools for home IoT devices, supported by a scalable and cost-effective assessment process, that consumers will intuitively trust and understand.

The private sector, in consultation with civil society and government experts, should devise an efficient and effective assessment and labeling approach for IoT devices so security-conscious consumers can make informed choices and create market incentives for security-by-design product development. Many commercially available IoT products were not designed with security in mind. These devices create a systemic risk for all members of the ecosystem, as well as placing consumers' privacy and security at risk. In an ideal world, consumers would prefer IoT products that also protect their security and privacy, but security-conscious consumers cannot easily identify IoT products that were designed to be secure. Without this information, their selection criteria are limited to the price and feature set.

The private sector is best suited to the creation and maintenance of lightweight and agile mechanisms, but can often benefit from government's convening power. The federal government should convene industry, civil society, and government stakeholders in a multistakeholder process to explore requirements for a viable process. This can build on initial successes of programs like NTIA's multistakeholder process on IoT upgradability and patching.[61] Stakeholders should consider whether a mechanism that relies on vendor assertion is viable and meets home consumer needs. Viability of such a mechanism could rely in part on existing prohibitions against commercial deception. For instance, the Federal Trade Commission could protect the integrity of the assessment mechanism by taking action against deceptive marketing (e.g., false compliance claims), understanding that security assurances in this space cannot offer similar guarantees compared to safety assertions that remain static over time. DHS could also support the assessment program through its existing awareness activities, such as STOP.THINK.CONNECT. (See Action 5.3).[62]

Widely recognized mechanisms, such as the NHTSA 5-Star Safety Rating and Energy Star programs, have successfully raised customer awareness and created markets for safe vehicles and energy-efficient appliances. However, the large number of different IoT devices and the relatively brief sales period for many of these devices (in comparison with cars and water heaters) indicates that a lighter weight and more agile mechanism will be required. Given the global nature of business today, the assessment scheme should be based on internationally recognized standards wherever possible. Further, any use of a security assessment and labeling approach would need to reflect the differences between safety assertions, which remain static over time, and security assertions, which cannot offer similar guarantees. DHS could complement such broadly applicable mechanisms by exploring opportunities regarding a certification regime that may be effective in supporting the needs of critical infrastructure.

There is also a role for subjective assessment of IoT devices and their usability. Consumer-oriented testing organizations often supplement feature-based analysis and repair histories with more subjective assessments of comfort or usability. Usability of management interfaces for security is a particularly difficult problem. By including thoughtful assessments of usability, consumer-oriented testing organizations can help consumers identify the products that are appropriate for their skill levels and backgrounds.

Action 5.2 The private sector should establish a voluntary labeling schemes for industrial IoT applications, supported by a scalable and cost-effective assessment process, to offer sufficient assurance for critical infrastructure applications of IoT.

Critical infrastructure and industrial applications of IoT present significantly higher risks to the nation than home applications. These devices are also deployed in very different environments, supported by professional administrators. The lightweight assessment mechanism envisioned in Action 5.1 would not offer a sufficient level of assurance for these customers, and additional features are likely to be required. Assessment features such as device authentication, hardware roots of trust, or managed update functions would require direct interaction with products, if not review of source code.

Examples of success for such a process exist in both the government and the private sectors. For example, NIST's Cryptographic Module Validation Program (CMVP) has leveraged independent testing laboratories to assess the security of cryptographic modules against the Federal Information Processing

[61] NTIA Multistakeholder Process on Internet of Things Upgradability and Patching. https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security (last updated November 7, 2017).

[62] Stop. Think. Connect., https://www.stopthinkconnect.org/ (last visited December 6, 2017).

Standards (FIPS) 140 standard for more than two decades. In the private sector, safety and certification company UL has a variety of certification and compliance schemes for both commercial and consumer markets, with more than 20 billion UL marks appearing on products in 2016.

The private sector should establish an efficient but robust evaluation process to ensure that IoT devices for these sectors offer enhanced resilience at an appropriate level of assurance. Establishing an evaluated products list will permit security-conscious enterprises to make informed choices and create market incentives for robust secure development lifecycle processes.

Action 5.3 Government should encourage the academic and training sectors to fully integrate secure coding practices into computer science and related programs.

As noted in Action 1.2, many common security vulnerabilities (such as buffer overflows) can be avoided or remedied during product development by applying the latest generation of powerful security development tools, such as fuzzers, static analyzers, and safe programming languages. While academic institutions, coding boot camps, and job retraining programs are creating a larger coding workforce, their graduates are rarely skilled in these languages or adept at using these development tools. Instead, students gain significant experience with software development tools that do not consider security, and software development methodologies that do not prioritize security, creating a bolt-it-on-later mindset among the software development workforce.

Companies that wish to improve coding practices may be deterred by an unprepared and sometimes resistant workforce—skilled coders can easily change jobs if they are not interested in learning the new practices, and can be challenging to replace. By teaching secure-by-design software methodologies and encouraging use of security-aware software development toolchains throughout the computer science curriculum, we can prepare our workforce to build higher quality software and increase acceptance of security-focused software development toolchains.

The federal government can facilitate these changes through existing relationships with academia and the training industry. In particular, the National Initiative for Cybersecurity Education (NICE), led by NIST, is an established partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. NICE should engage with academia and the private sector to incorporate secure-by-design principles and supporting tools at every step in the course of study. The FTC hosts an annual PrivacyCon conference, which provides a showcase for privacy and security work by academics and security researchers.[63]

Action 5.4 The academic sector, in collaboration with the National Initiative for Cybersecurity Education, should establish cybersecurity as a fundamental requirement across all engineering disciplines.

As IT is integrated into the full range of products and services, cybersecurity threats are experienced from new classes of products. Product designers are often unaware of the risks that can be introduced when integrating IT into traditional product lines. For example, closed circuit television (CCTV) cameras have been available commercially since 1949, but only recently evolved into Internet-connected devices. In 2016, the Mirai botnet compromised more than 100,000 CCTV cameras to support DDoS attacks. In

[63] *See* Federal Trade Commission, *PrivacyCon 2018*, https://www.ftc.gov/news-events/events-calendar/2018/02/privacycon-2018 (last visited December 6, 2017).

other cases, Internet-connected cameras used as baby monitors have been hacked by exploiting default administrative passwords, violating the owners' privacy.[64]

To ensure that product designers are aware of the risks introduced into operational technology, academic institutions teaching engineering and related disciplines should integrate basic cybersecurity into the required curriculum. As above, NICE should engage with academia and the private sector to incorporate principles into the course of study for engineering and related disciplines.

Action 5.5 The federal government should establish a public awareness campaign to support recognition and adoption of the home IoT device security profile and branding.

To achieve impact, the home IoT device security profile must be recognized and preferred by security-conscious consumers, enhancing the resilience of home networks where the devices are installed and establishing market incentives for security-conscious vendors. The federal government has a long history of public awareness campaigns to address a wide variety of topics: preventing forest fires, importance of seatbelts, and the importance of HIV testing. The Stop.Think.Connect. campaign is a DHS-sponsored national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The federal government should consider leveraging Stop.Think.Connect. or establishing a complementary public awareness campaign to alert home users and small organizations to socialize the importance of the home IoT device profile and educate them on how to identify compliant products. More generally, enhanced user awareness of cybersecurity risk is critical to a resilient ecosystem, and government should increase its strategic engagement and convening power with targeted user communities and civil society to improve security adoption and awareness.

[64] *See* Darlene Storm, *Hacker Hijacks Wireless Foscam Baby Monitor, Talks and Freaks Out Nanny*, Computerworld (Feb. 2, 2015, 12:09 PM PT), https://www.computerworld.com/article/2878741/hacker-hijacks-wireless-foscam-baby-monitor-talks-and-freaks-out-nanny.html.