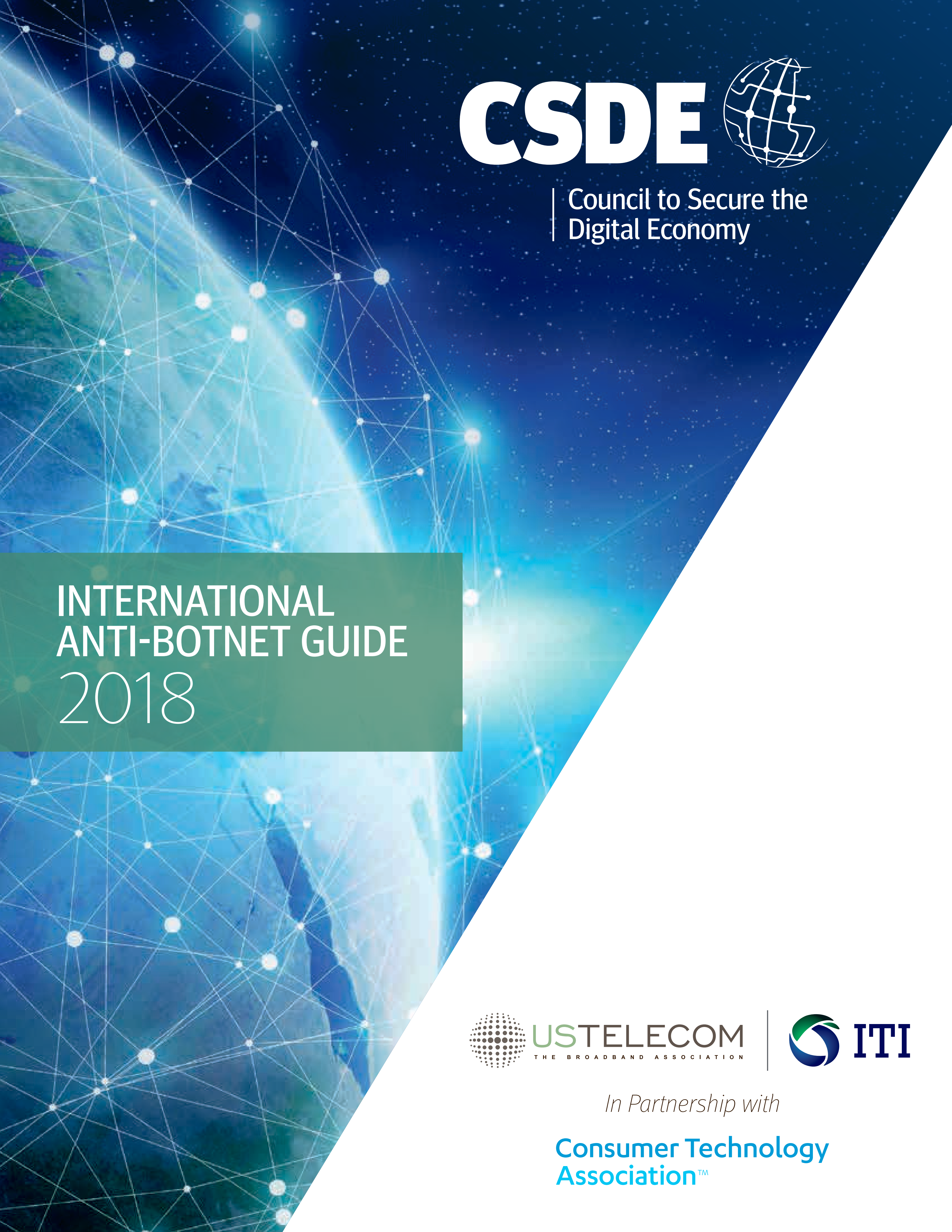


CSDE

Council to Secure the
Digital Economy

INTERNATIONAL ANTI-BOTNET GUIDE 2018

USTELECOM
THE BROADBAND ASSOCIATION

ITI

In Partnership with

Consumer Technology
Association™

NOTICE

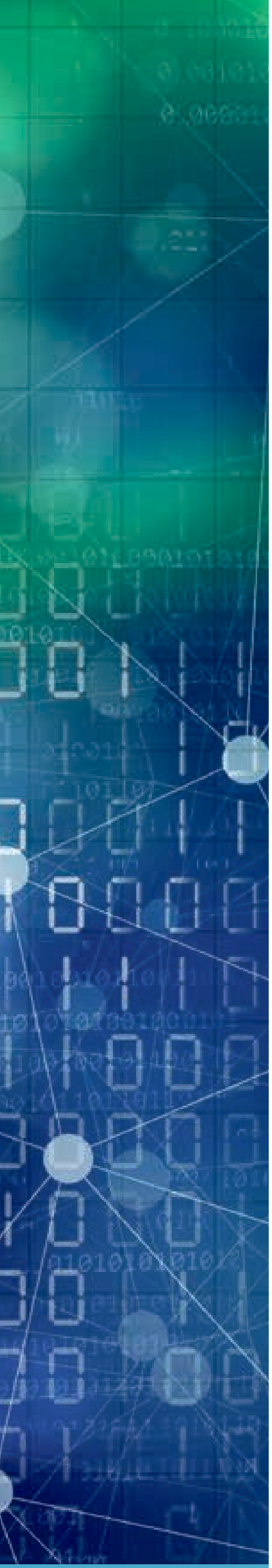
The International Anti-Botnet Guide was developed to facilitate the mitigation of botnets and other automated, distributed threats through voluntary participation and collaboration among disparate stakeholders throughout the global internet and communications ecosystem. The Guide provides information and encouragement to Information and Communications Technology (ICT) stakeholders about affirmative measures to implement towards this goal as they deem appropriate, based upon their individual circumstances and their relationships with each other.

The Guide highlights impactful voluntary practices for each segment of the ICT sector, ranging from "baseline" to "advanced." While the industry leaders who have developed this Guide recognize that no combination of measures can guarantee the elimination of all threats and risks, they believe these practices, both baseline and advanced, present a valuable framework for ICT stakeholders to reference in identifying and choosing practices of their own to mitigate the threats of automated, distributed attacks. The Guide recognizes that different ICT stakeholders face different challenges, considerations, and priorities as they implement security measures. Accordingly, the practices identified in this Guide, and the Guide as a whole, are tools that ICT stakeholders should implement according to their circumstances; they are not requirements or mandates, or otherwise compulsory in any way.

Many of the practices and technologies discussed in this document are already being used by large-scale enterprises to protect their networks and systems, ranging from contracting for deep packet inspection (DPI) from network service providers to prohibiting the use of devices that do not have sufficient built-in security measures. However, the implementation of these capabilities in the wider consumer space has broader policy implications. For example:

- Advanced capabilities such as DPI of IP traffic, while useful in certain contexts, could have significant implications for individual privacy if deployed on public networks.
- If required by governments to meet other policy objectives, filtering of public network traffic based on IP addresses and other means may also have implications for the free flow of information.
- Enterprises have skilled IT staff who negotiate detailed requirements with their suppliers and incorporate cost-benefit analyses in decisionmaking. Such dynamics do not exist in the consumer space, where the cost-benefit analysis can differ significantly from that of a large scale enterprise. For consumers, cost and consumer protection issues will need to be evaluated on a different risk management scale.
- Devices that are deemed to have insufficient security capabilities cannot simply be banned from sale in a given country on an ad hoc basis without considering international trade implications and other local regulations.

COPYRIGHT STATEMENT



Contents

01 Executive Summary

The members of the Council to Secure the Digital Economy (CSDE) and the Consumer Technology Association (CTA)™ span the entirety of the complex global internet and communications ecosystem, providing infrastructure, software, and devices that benefit a significant portion of the world's consumers, small businesses, large private enterprises, governments, and non-profits — collectively, the global digital economy.

The companies that contributed to this Guide were among the earliest adopters of voluntary practices to secure the ecosystem from cyber threats. Meanwhile, the technology sector has benefited from secure-by-design practices, managed security services, and lifecycle support supplied by global providers of hardware, software, devices and systems, and related services. Still, challenges abound for infrastructure providers, software developers, device and systems manufacturers, systems installers, and enterprises of all types.

The CSDE's International Anti-Botnet Guide, developed in close partnership with CTA, draws on the diverse global perspectives, practices, and experiences of these stakeholders to address a persistent and increasing challenge to the global digital economy: botnets and other automated, distributed threats.

Activating Shared Responsibility to Secure the Global Digital Economy. The digital economy has been an engine for commercial growth and quality-of-life improvements across the world. But no single stakeholder — in either the public or private sector — controls this system. Rather, securely managing the opportunities presented by this growth is the challenge and responsibility of every stakeholder in the Information and Communications Technology (ICT) community.

In recent years, however, botnets have become particularly and increasingly damaging and costly to the digital economy. Botnets are large networks of compromised, internet-connected computers and devices that malicious actors can command to commit distributed denial of service (DDoS) attacks, propagation of ransomware, phishing attacks, and disinformation campaigns amplifying inauthentic social media, and other malicious acts.[1] Unfortunately, as the number of connected people, businesses, and devices grows, so does the potential for these malicious attacks. Today, the destructive potential of botnets has increased exponentially as they attack and leverage the billions of Internet of Things (IoT) devices, estimated to reach 20 billion connected devices by 2020. With this substantial and growing attack surface, it is no coincidence that the global cost of cyber-crimes is expected to reach trillions of dollars. Botnets are the industrial-scale driver of these losses.

In fact, the botnet threat is more severe today than at any previous point in history. Huge, high-profile attacks on major organizations have been recently documented, while an undercurrent of smaller, lower profile attacks have resulted in continuous yet unknown harm. These developments inflict direct, tangible costs — amounting to billions of dollars — on the digital economy. The intangible costs are just as detrimental, as these threats undermine fundamental confidence and trust in the digital economy.

This Guide aims to reverse these trends. While the developers of this Guide strongly support the important role that governments play in convening a diverse ecosystem, the imposition of prescriptive, compliance-focused regulatory requirements will inhibit the security innovation that is key to staying ahead of today's sophisticated threats. Moreover, earlier policy efforts were based on utopian solutions to these threats, premised on the notions that internet service providers (ISPs) can simply shut down all botnets, or that manufacturers can make all devices universally secure. Instead, dynamic, flexible solutions that are informed by voluntary consensus standards, driven by market demands, and implemented by stakeholders throughout the global digital economy, are the better answer to these evolving systemic challenges.

To enable such solutions and encourage the sharing of responsibility among all stakeholders, this Guide sets forth a set of *baseline practices* that various stakeholders should implement; further, it highlights additional *advanced capabilities* that are presently available but underutilized. Widespread implementation of the security practices featured in this Guide will dramatically reduce botnets and help secure the global digital economy. The Guide provides real-world, presently available solutions to a global challenge that cannot be met by one stakeholder set or one country alone or by any governmental mandate. The Guide is informed by an ongoing collaboration with companies across multiple industries and countries to dramatically reduce the botnet threat, and by an analysis of rapidly evolving global threats and vulnerabilities, as well as increasingly capable and determined adversaries.

The Guide is premised on, and affirmatively seeks to advance, the following core security principles:

- Security demands dynamic, flexible solutions that are driven by powerful global market forces and are as nimble and adaptable as the cyber threats that need to be mitigated, rather than regulatory compliance mechanisms that differ by local or national jurisdiction.
- Security is a shared responsibility among all stakeholders in the internet and communications ecosystem. Government and industry stakeholders should promote solutions that increase responsibilities among all players, rather than seeking facile solutions among certain select components or stakeholders.
- Security relies on mutually beneficial teamwork and partnership among governments, suppliers, providers, researchers, enterprises, and consumers, through collective action against bad actors and rewards for the contributions of responsible actors.

  These principles are the foundation of the new approach to botnet mitigation that circumstances demand.

The International Anti-Botnet Guide: Summary of Practices and Capabilities. The complexity and diversity of the “system of systems” comprising the internet and associated communications ecosystem makes it impossible to provide a set of guidance that uniformly applies to all stakeholders. The Guide groups these diverse components based on five constituent types of provider, supplier, and user stakeholders: (1) Infrastructure, (2) Software Development, (3) Devices and Device Systems, (4) Home and Small Business Systems Installation, and (5) Enterprises. For each of these components, the Guide lays out baseline practices that all such stakeholders should aspire to meet, as well as advanced capabilities that are presently available — if underutilized — in the marketplace. These practices and capabilities, summarized briefly below, are the core of this Guide.

1. ***Infrastructure.*** For purposes of this Guide, “infrastructure” refers to all systems that enable connectivity and operability — not just to the physical facilities of providers of internet service, backbone, cloud, web hosting, content delivery, Domain Name System, and other services, but also software-defined networks and other systems that reflect the internet’s evolution from tangible things to a digital concept. We recommend baseline practices and advanced capabilities for infrastructure to include:
   - **Detect Malicious Traffic and Vulnerabilities**
   - **Mitigate Against Distributed Threats**
   - **Coordinate with Customers and Peers**
   - **Address Domain Seizure and Takedown**

2. ***Software Development.***[2] Software is an increasingly ubiquitous element of every other component of the ecosystem. There are a wide variety of complex development processes and interdependencies that drive software innovation and improvement. We recommend that software generally consist of baseline practices and advanced capabilities to include:
   - **Secure-by-Design Development Practices**
   - **Security Vulnerability Management**
   - **Transparency of Secure Development Processes**

3. ***Devices and Device Systems.***[3] An individual connected device (or “endpoint device”) may itself consist of multiple components, including hardware modules, chips, software, sensors or other operating components. Beyond the individual device itself are multiple additional layers of connectivity that constitute a highly dynamic new market — including for security innovation. For the endpoint “things” in the IoT, and the applications and services that come with them, we recommend baseline practices and advanced capabilities to include:
   - **Secure-by-Design Development Practices**
   - **Roots of Trust**
   - **Product Lifecycle Management Including End-of-Life**
   - **Security-Focused Toolchain Use**

4. ***Home and Small Business Systems Installation.***[4] Homes and small businesses benefit from connected devices in several categories. These systems can be installed by do-it-yourself home and business owners, or by professionals: integrators, alarm contractors, and others. Drawing heavily from The Connected Home Security System,[5] we recommend baseline practices and advanced capabilities to include:
    - **Authentication and Credential Management**
    - **Network Configuration**
    - **Network Hardware Management**
    - **Security Maintenance**

5. ***Enterprises.***[6] As major owners and users of networked devices and systems, including an exponentially increasing number of IoT device systems, enterprises of all kinds — government, private sector, academic, non-profit — have a critical role to play in securing the digital ecosystem. For enterprises, we recommend baseline practices and advanced capabilities to include:
    - **Secure Updates**
    - **Real-time Information Sharing**
    - **Network Architectures that Securely Manage Traffic Flows**
    - **Enhanced DDoS Resilience**
    - **Identity and Access Management**
    - **Mitigating Issues with Legacy and Pirated Products**

Next Steps and Implementation. The publication of this Guide is only a first step. Next, we will strategically engage a broad set of stakeholders, including governments of like-minded countries, to promote the Guide's baseline practices and advanced capabilities. Further, we will update, publish and promote a new version of the Guide annually.

> **The digital economy has been an engine for commercial growth and quality-of-life improvements across the world, creating jobs and opportunities on every continent. It may already represent 20% of global economic value.**

02 Introduction

The members of the Council to Secure the Digital Economy (CSDE)[7] and the Consumer Technology Association[8] (CTA)™ cover the entirety of the complex global internet and communications ecosystem. These organizations count among their members companies that provide the human and technical systems that create, manage, and install connectivity capabilities, software, and devices that benefit a significant portion of the world's consumers, small businesses, large private enterprises, governments, and non-profits — collectively, the global digital economy. The CSDE's International Anti-Botnet Guide, developed in close partnership with CTA, draws on the diverse international perspectives of these stakeholders, as well as their influential practices and real-world actions, to address a persistent and increasing challenge to that digital economy: botnets and other automated, distributed threats.[9]

Overview of the Challenge. The digital economy has been an engine for commercial growth and quality-of-life improvements across the world, creating jobs and opportunities on every continent. By some estimates, it may already represent 20% of global economic value.[10] While GDP alone cannot capture the full contributions of the digital economy to global economic value — not all value provided digitally involves a commercial transaction — *The Wall Street Journal* reports that the digital economy was worth $11.5 trillion in 2016 and may increase to $23 trillion, nearly a quarter of global GDP, by 2025.[11] The digital economy's growth is being fueled continuously by business and consumer adoption of new and emerging technologies.[12] Securely managing the opportunities presented by this impressive growth is the challenge and responsibility of every stakeholder in the Information and Communications Technology (ICT) community.

In recent years, however, botnets have become particularly and increasingly damaging and costly to the digital economy. They are able to propagate malware,[13] conduct denial of service attacks,[14] and spread corrosive disinformation artificially on social media.[15] A single botnet can now include more than 30 million "zombie" endpoints and allow malicious actors to profit six figures per month.[16] More systems are vulnerable today than ever before, due simply to the tremendous and otherwise promising growth of the digital economy itself — particularly regarding the rapid deployment of billions of Internet of Things (IoT) devices, estimated to reach 20 billion connected devices by 2020.[17] The benefits of this connected economy are revolutionizing businesses and consumer activities for the good, and the companies that have developed this Guide are innovating new security measures as they deploy devices. Nevertheless, insecure devices continue to stream into the marketplace without systems in place that are designed to secure them.[18] Moreover, it is now possible for relatively unskilled malicious actors to rent a powerful botnet to use for large-scale nefarious activities.[19]

These developments inflict direct, tangible costs on the digital economy. For example, since 2017, malware has spread across Europe, Asia, and the Americas, causing more than $10 billion in damage.[20] It is estimated that over the next five years cyber-crimes alone will globally cost businesses a cumulative total of $8 trillion (in fines, loss of business, remediation costs, etc.).[21]

> **“Combating botnets requires cross-border and multidisciplinary collaboration, innovative technical approaches, and the widespread deployment of mitigation measures that respect the fundamental principles of the Internet.”**
>
> **- THE INTERNET SOCIETY**

The intangible costs are just as detrimental, as these threats undermine fundamental confidence and trust in the digital economy.

Strategic Posture and Goals. We aim to reverse these trends. While we recognize and support the important convening role that governments can play in helping to channel the activities of the diverse players in the ecosystem, we also believe that compliance-based regulatory requirements actually inhibit the security innovation that is required to stay ahead of today’s sophisticated threats. In other words, not only are prescriptive regulatory requirements rarely effective, but they are in fact usually counterproductive to the goal of security.[22] Dynamic, flexible solutions that are informed by voluntary consensus standards, driven by market demands, and implemented by stakeholders throughout the global digital economy are the better answer to evolving systemic challenges like malicious botnets that threaten all players in this complex ecosystem.

Therefore, this Guide seeks to empower responsible participants in the digital economy to secure its future and leverage its full potential. We believe that active collaboration and collective action will be commercially beneficial for all stakeholders, large and small, over the long term. To that end, this Guide may be used to increase the resilience of the internet and communications ecosystem and enhance the transactional integrity of the underlying digital infrastructure. The Guide urges all stakeholders in this global digital marketplace to implement a set of baseline tools, practices, and processes; further, it highlights additional advanced capabilities that are presently available — but perhaps still underutilized. Widespread implementation of the security practices featured in this Guide will dramatically reduce botnets and help secure the global digital economy.

Methodology and Next Steps. The companies contributing to this Guide have undertaken a comprehensive review of practices and materials that showcase technology and tools that are known to be effective for combating automated, distributed attacks such as botnets; they also researched reports from governments and international bodies and consulted outside experts and sources from industry, academia, and civil society.[23] But to be clear, publication of this Guide is only a first step. Next, we will strategically engage a broad set of stakeholders, including governments of like-minded countries, to promote the Guide’s baseline practices and advanced capabilities. Further, we will update, publish, and promote a new version of the Guide annually.

03 Botnets: Addressing Automated, Distributed Threats in a Diverse Internet Ecosystem

The most prominent category of automated, distributed threats to the global internet and communications ecosystem is botnets — large networks of compromised internet-connected computers and devices that communicate with servers that have command-and-control capabilities.

Botnets spread themselves globally through malware that scans the internet for insecure networks, computers, and other connected devices. When a botnet has compromised a sufficient number of devices, criminals and other bad actors can command them to commit a broad variety of nefarious acts such as distributed denial of service (DDoS) attacks, propagation of ransomware, phishing attacks, and disinformation operations that artificially amplify inauthentic social media posts.[24]

The botnet threat is more severe today than at any previous point in history. In the early 2000s, criminals mainly used botnets for rudimentary denial of service (DoS) attacks that flooded and overwhelmed targeted websites and network activities with artificial internet traffic. As time moved on, however, their capabilities grew. By infecting large numbers of devices with malware, hackers found that they were able to conduct malicious activities on a much larger scale. In 2007, a botnet called "Storm Worm" was found to have gathered nearly 50 million computers into its ranks, using them to commit crimes such as stock price fraud and identity theft. In 2009, one botnet was found to be sending an incredible 74 billion spam emails every day.[25] And in 2011–2013, an attacker utilized botnets to conduct a campaign of DDoS attacks against North American banks, sending waves of internet traffic to their websites from botnet nodes all over the world.[26]

Today, criminals use large botnets for all sorts of cybercrimes, from cryptocurrency mining to DDoS attacks, such as 2016's historic Mirai botnet attack on the DNS provider Dyn. The 2016 Mirai botnet malware spread using a list of default login credentials to gain access to nearly 400,000 endpoint devices such as CCTV video cameras and digital video recorders, without owners noticing or internalizing any of the economic consequences of their devices being infected.[27] The attack — which by volume of botnet-driven traffic was ***four*** times the volume of the earlier attacks against major banks — temporarily disabled user access to key online platforms and services, causing serious problems for the many users who depended on the online services of companies such as Airbnb, Amazon.com, BBC, CNN, and Netflix, to name a few.[28]

While the majority of botnets do not reach the scale of Mirai,[29] many smaller botnet attacks are able to shut down websites and services, spread ransomware, and drive disinformation on social media. Unfortunately, smaller attack capabilities have become much more accessible to criminals lacking the technical knowledge to build their own botnets. Online marketplaces found on the dark web allow novice hackers to buy the toolkits to design unique botnets that meet their individual needs — called "Malware as a Service" (MaaS). If the criminal customer does not want to develop or buy a botnet, he or she can rent one for as little as $0.66 cents a day.[30] And the criminal can simply purchase the function — say, a DDoS attack — for as little as $20.[31] It is a thriving and innovative marketplace. Shortly after the Mirai attacks, for instance, the botnet's creator published the Mirai source code online, and since then many other aspiring hackers have made variants of the original Mirai code.

Malicious actors are constantly finding new uses for botnets. For example, hackers used botnets in an attempt to revive the infamous WannaCry ransomware, which incapacitated more than 200,000 computer systems in over 150 countries, forcing banks, hospitals, universities, and other institutions to shut down or pay ransom money to criminals.[32] The WannaCry outbreak receded when a security researcher realized the malware was querying an unregistered domain. Registering the domain had the effect of a "kill switch" that shut down the botnet.[33] Hackers have used "copycats of the Mirai botnet" to attack this domain relentlessly with the goal of bringing the temporarily defeated ransomware back to life.[34] Meanwhile, an even more sophisticated piece of ransomware than WannaCry — Petya — has emerged to wreak havoc across the globe, and malware based on Petya (called NotPetya) has already cost more than $10 billion in damages.[35]

> **The capabilities of malicious botnets threaten to undermine fundamental confidence and trust in the digital economy.**

Unfortunately, as the number of connected people, businesses, and devices grows, so does the potential for, power of, and profits from larger malicious attacks. As described above, the total number of connected devices in use worldwide is in the billions, and not coincidentally, the global cost of cyber-crimes is expected to be in the trillions. Botnets are the industrial-scale driver of this problem. Besides the obvious economic losses, the capabilities of malicious botnets threaten to undermine fundamental confidence and trust in the digital economy. That outcome defies quantification, but its negative impact can have a debilitating effect, just as concerns about pollution threaten our confidence in the air we breathe and the water we drink.

The fundamental challenge of addressing botnets in the highly diverse, complex, and interdependent global internet ecosystem is that the essential nature of the internet is non-hierarchical and hyper-connected. No single stakeholder — government or private sector — controls this system, and yet we rely on it to connect all of us. Fighting malicious botnets is the classic "tragedy of the commons" challenge: If everybody has a stake in the internet commons and is inescapably connected to it, but nobody controls, then who is responsible for cleaning up the malicious botnets that threaten basic functions that everybody relies on?

The answer is that all stakeholders must take responsibility — and not just for altruistic purposes of cleaning up the commons. Every entity in the ecosystem has a self-interested stake in reducing malicious botnets. Botnets are used to attack the internet on which all ICT offerings rely, and being involved in a botnet attack hurts the companies involved either by direct impact on execution or harm to reputation.

Previous Efforts to Address this Ecosystem-Wide Challenge

The companies responsible for this Guide have been among the earliest adopters of voluntary practices to secure the ecosystem from botnets. For example, in 2012, leaders of the U.S. communications sector developed the Anti-Botnet Code of Conduct for ISPs, taking meaningful action toward rooting out botnets through education, detection, notification, remediation, and collaboration. Meanwhile, the technology sector has benefited from secure-by-design practices, managed security services, and lifecycle support supplied by global providers of hardware, software, devices and systems, and related services.

Still, challenges abound throughout the ecosystem:

- Many ISPs and other infrastructure providers with advanced capabilities are continually driving the marketplace toward a state of increased security in order to mitigate the botnet threat. As the size and complexity of botnets increase, companies that operate infrastructure networks have added network capacity to protect customers from increasingly large attacks. However, there is more that all stakeholders can do to operate efficiently in the ecosystem — and smaller providers often need guidance and resources for getting up to the baseline.
- Software is integral to all global commerce and government processes. The diverse stakeholders in the digital economy increasingly rely on secure software. This reliance has incentivized bad actors to develop increasingly sophisticated exploits. In response, responsible companies have developed secure practices for software development and set basic security goals for each stage of the product lifecycle. These are practices that smaller developers can emulate.
- The astounding innovations in the development, deployment, and use of connected device systems is a double-edged sword, introducing billions of new internet-enabled devices to the world and just as many new entry points for cybercriminals to exploit. As indicated above, many of these devices simply were not designed or deployed with security in mind — and they are not deployed within systems that are able to mitigate their individual vulnerabilities.
- Computers and connected devices in a home or enterprise should be secured throughout the entire lifecycle of the device — perhaps most importantly, upon the initial installation and configuration of the device. Proper installation and configuration are still too rare, however, and therefore products often do not achieve their best available security performance.
- Enterprises of all types — in the public and private sectors – are both the victims and the host propagators of botnets and other automated, distributed threats. These enterprises have much to gain from adopting security solutions like those increasingly available in the marketplace.

A SINGLE BOTNET
CAN NOW INCLUDE
MORE THAN
30
MILLION
“ZOMBIE” ENDPOINTS
AND ALLOW MALICIOUS
ACTORS TO PROFIT
SIX FIGURES PER MONTH

> **Security demands dynamic, flexible solutions that are driven by powerful global market forces and are as nimble and adaptable as the cyber threats that need to be mitigated.**

Against this backdrop the common mistake of past policy efforts has been their narrow focus on one or two components of the ecosystem — the policymaking equivalent of trying to cull a forest of diseased trees simply by cutting the branches closest in reach. More likely than not, the result will be a forest still full of diseased trees. Likewise, the mitigation of botnets requires a more thoughtful, holistic approach. The various parts of this complex ecosystem must — for their individual and collective good — deepen and sharpen their understanding of their own responsibilities and how they complement those of others. And in cases where the lines currently are unclear or unknown, stakeholders must work together to clarify them. Absent such work, strategies for combating botnets will revert to the fallacy of utopian policy solutions focused on just one or two pieces of the puzzle — for instance, that ISPs should simply shut down all botnets, or that billions of devices should be made universally secure, or that consumers should become omniscient users of technology.

Such simplistic solutions have failed thus far and are unlikely to be any more successful in the future. Instead, this intricate system composed of billions of human and automated components throughout the private sector consumer and enterprise marketplaces, academia, civil society, and governments worldwide must implement mitigation methods at every level to increase its security. That is what this International Anti-Botnet Guide aims to do.

What is Different Now?

This Guide provides real-world, presently available solutions to a challenge in today's marketplace that cannot be met by any government requirement(s) or a single country alone. We are working with global companies across multiple industries to reduce the botnet threat dramatically. We developed this Guide, informed by analysis of rapidly evolving global threats, ecosystem-wide vulnerabilities, and increasingly capable and determined adversaries, with the following consensus guiding principles in mind:

- Security demands dynamic, flexible solutions that are driven by powerful global market forces and are as nimble and adaptable as the cyber threats that need to be mitigated, rather than regulatory compliance mechanisms that differ by local or national jurisdiction.
- Security is a shared responsibility among all stakeholders in the internet and communications ecosystem. Governments and industry stakeholders should promote solutions that increase responsibilities among all players, rather than seeking facile solutions among certain select components or stakeholders.
- Security relies on mutually beneficial teamwork and partnership among governments, suppliers, providers, researchers, enterprises, and consumers, built on a framework that takes collective action against bad actors and rewards the contributions of responsible actors.

04 Overview of the Global Internet and Communications Ecosystem

As noted above, the digital economy runs on — and was made possible by — a complex global internet and communications ecosystem that is comprised of numerous systems, each of which is highly complex in its own right and highly interdependent on all of the others. And all of these different components constitute part of the ecosystem's vulnerability to — and its resilience against — the threats posed by botnets and other automated, distributed attacks.

The complexity and diversity of the "system of systems" comprising the internet and associated communications ecosystem makes it impossible to provide a set of guidance that uniformly applies to all stakeholders. Various prominent government and private sector reports have defined and described the internet and communications ecosystem using similar yet different taxonomies that were tailored to the purposes and goals of each forum.[36] Rather than serving as competing visions of how the ecosystem should be understood, these definitions complement and reinforce each other.

The digital economy was worth $11.5 trillion in 2016 and may increase to $23 trillion, nearly a quarter of global GDP, by 2025

This Guide is no exception. We group the ecosystem's components in a manner that facilitates the identification and implementation of anti-botnet practices among its constituent groups of stakeholders. Specifically, the Guide is organized around the following five types of providers, suppliers, and users:

1. Infrastructure
2. Software Development
3. Devices and Device Systems
4. Home and Small Business Systems Installation
5. Enterprises

To be sure, any effort to define this complex ecosystem carries some risk of being underinclusive in some way, whether actual or perceived. For instance, experience may reveal that none of the five categories listed above can reasonably accommodate some ubiquitous platforms (e.g., large social media platforms) that involve some combination of categories. For that reason, this taxonomy should be viewed flexibly with the expectation that the boundaries between systems will continue to evolve.

05 Practices and Capabilities of Components of the Ecosystem

A. INFRASTRUCTURE

For purposes of this Guide, “infrastructure” refers to all systems that enable connectivity and operability — not just to the physical facilities of providers of internet service, backbone, cloud, web hosting, content delivery, Domain Name System, and other services, but also software-defined networks and other systems that reflect the internet’s evolution from tangible things to a digital concept. We recommend baseline practices and advanced capabilities for diverse infrastructure in the modern internet and communications ecosystem.

Types of Infrastructure

Internet Service Providers

An internet service provider (ISP) is an organization that provides customers a means to access the internet using technologies such as cable, DSL (digital subscriber line), dial-up, and wireless. ISPs are connected to one another through network access points, public network facilities found on the internet backbone. ISPs use these vast systems of interconnected backbone components to transfer information across long distances within seconds. ISPs may provide services beyond accessing the internet including web-site hosting, domain name registration, virtual hosting, software packages, and e-mail accounts. Many ISPs offer services designed to reduce botnets, including managed security solutions whereby the provider takes an active role in mitigating threats to customers. Most broadband ISPs provide antivirus as part of their offering, and many notify infected customers without any additional charges.

Internet Backbone Providers

The internet’s backbone is a collection of vast, connected computer networks that are generally hosted by commercial, government, academic, and other network access points. These organizations typically have control over large high-speed networks and fiber optic trunk lines, which are essentially an assortment of fiber optic cables bundled together in order to increase capacity. They allow for faster data speeds and larger bandwidth over long distances, and they are immune to electromagnetic interference. Backbone providers supply ISPs with access to the internet and connect ISPs to one another, allowing ISPs to offer customers high speed internet access. The largest backbone providers are called “tier 1” providers. These providers are not limited to country or region and have vast networks that connect countries across the world. Some tier 1 backbone providers are also ISPs themselves and, due to their size, these organizations sell their services to smaller ISPs.

DNS Providers

The Domain Name System (DNS) is essentially an address book of domain names associated with IP addresses copied and stored on millions of servers around the world. When a user wishes to visit a website and types the domain name into the search bar, the computer sends that information to a DNS server. This server (also referred to as a resolver) is usually run by the user's ISP. The resolver then matches the domain name with an IP address and sends the corresponding IP address back to the user's browser which then opens a connection with the webserver.

DNS providers are organizations that offer such DNS resolution services. They provide the most common DNS functions such as domain translation, domain lookup, and DNS forwarding. DNS providers also routinely update their name servers to provide the most current information.

Content Delivery Networks

A content delivery (or distribution) network (CDN) is a geographically dispersed network of data centers and proxy servers. CDN is a term used to describe many different types of content delivery services such as: software downloads, web and mobile content acceleration, and video streaming. CDN vendors may also cross over into other industries like cybersecurity with DDoS protection and web application firewalls (WAF). CDNs were designed to solve a problem known as latency, the delay that occurs between the time that a user requests a web page to the moment that its content appears onscreen. The duration of the delay typically depends on the distance between the end user and the hosting server. To shorten this duration, CDNs reduce that physical distance and improve site rendering speed and performance by storing a cached version of its contents in several locations, known as points of presence or PoPs; each PoP connects end users within its proximity to caching servers responsible for content delivery. By storing a website's content in many places at once, a company can provide superior coverage to far away end users.

Cloud and Hosting Providers

Internet hosting services enable customers to make content accessible on the internet to people and organizations throughout the world. In recent years, the increased adoption of cloud hosting services, which use remote servers hosted online instead of a local server or a personal device, has given customers access to scalable and more secure hosting solutions. Software, infrastructure, and platforms hosted on the cloud can be accessed on a subscription basis and enable customers to perform a wide variety of computing functions. Because cloud networks are decentralized, they can typically withstand the disruption of numerous network components. This architectural feature makes the cloud more resilient to highly distributed botnets and provides additional mitigation capabilities. In essence, cloud services provide an extra layer of security outside of the infrastructure provided by an ISP. This layer of protection becomes increasingly useful as the scale of botnet attacks increases. Because the cloud is upstream relative to ISPs from the target of an attack, it can mitigate the problem closer to the attack source. Cloud security services complement and do not diminish the role of ISPs in botnet mitigation.

> **Certain baseline practices have already been proven to reduce the impact of botnet-driven attacks such as DDoS attacks and should be implemented throughout the ecosystem.**

Baseline Practices and Advanced Capabilities for Infrastructure

CSDE members take critical steps to increase the resilience of their own networks, their customers' networks, and the global ecosystem against botnets. Experts in government and industry have observed that because of the complexity of the ecosystem, no single tool will always be effective to mitigate threats,[37] which means that industry must retain enough flexibility to adapt to emerging threats and new technologies and tools. However, certain baseline practices have already been proven to reduce the impact of botnet-driven attacks such as DDoS attacks and should be implemented throughout the ecosystem.[38] Below, we identify baseline practices as well as more advanced capabilities that industry leaders use to secure the ecosystem against distributed threats.

1. DETECT MALICIOUS TRAFFIC AND VULNERABILITIES

The first step in mitigating distributed threats such as botnets is identifying the assets that need to be defended from attacks and the potential vulnerabilities (i.e. attack surfaces) that potentially expose these assets. Moreover, companies should stay informed about the latest exploits (i.e. attack vectors) for each identified vulnerability.

Providers can leverage trusted third-party data feeds and information-sharing mechanisms, both within their industry and across sectors. Moreover, government information-sharing mechanisms in many countries enable information to be shared between the public sector and the private sector rapidly at machine speed.[39]

Summary of Baseline Detection Practices: Providers check for known types of malware in databases that are updated regularly. A responsible company may contribute to detection efforts by sharing information on new malware with security vendors and researchers in a timely manner.

Summary of Advanced Detection Capabilities: Companies with access to greater resources may have a dedicated staff of security researchers that can analyze heuristics and anomalous behaviors to detect malware. The researchers' findings can be shared with other stakeholders.

a) Signature analysis

When security experts encounter malware, they search for a unique pattern or "signature" (for example, a part of the malware's code and the exploit code). Signature-based analysis can then be used by anyone with access to an updated database of malware signatures so that the threat can be identified regardless of where it is encountered. This sort of analysis is common in antivirus software and intrusion detection systems, and can be used to detect most malicious threats on a network. Although signature analysis is commonly used, more sophisticated malicious actors can limit the usefulness of this technique by changing the specifics of malware every time it spreads. Like a real virus, malware can adapt and evolve as it moves from host to host.[40] A more obvious limitation of signature analysis is that it requires foreknowledge of the malware, which means that the effectiveness of signature analysis depends on timely updates and information-sharing throughout the ecosystem. Ideally, signature analysis should be combined with other types of analysis, such as heuristic or behavioral analysis discussed below, in order to overcome the inherent limitations of this technique.[41]

Baseline Practices: Providers should ensure their signature databases are up-to-date and they should contribute to information-sharing of malware.

Advanced Capabilities: Providers can combine signature analysis with analysis of code heuristics (described below) and network traffic behaviors (also described below) to achieve better results.

b) Heuristic analysis

Heuristic analysis detects malware by examining code for known signs of trouble. The code does not have to exactly match known malware to be flagged as potentially malicious. Heuristic analysis looks for many different clues in determining whether code is suspicious. In static heuristic analysis, potentially malicious code is compared to the code of malware in a database and if there are sufficient similarities then the code is flagged. Although the possibility of false positives exists, heuristic analysis is far more effective than signature analysis at combating unknown and evolving threats. Sometimes, in order to deconstruct code safely, scientists store suspicious code that they believe to be malware inside a virtual machine called a “sandbox,” thereby preventing it from spreading to other hosts. This is known as dynamic heuristic analysis.[42]

Advanced Capabilities: Providers can detect previously unknown threats by using a combination of both static and dynamic heuristic analysis. Providers with teams of researchers can analyze suspicious code inside a sandbox to determine effective mitigation strategies, which can be shared with other stakeholders in the ecosystem.

c) Behavioral analysis

Whereas signature analysis and heuristic analysis both focus on malware code, behavioral analysis focuses on the “symptoms” of malware infection. When network traffic indicates unexpected behavior, it may not be clear at first what is causing the change in behavior. However, there are known indicators that a piece of software may be malicious, for example when it attempts to gain elevated privileges or interacts in an anomalous manner with other software or files on a system. Often, behavioral analysis is analogized to the medical profession: a doctor can often tell when someone is sick even before knowing exactly what the problem is. Behavioral analysis complements other types of analysis by discovering unknown threats that have not yet been identified and therefore have no known signatures.[43]

Advanced Capabilities: Providers can use algorithms to detect anomalous traffic patterns and leverage institutional knowledge or if necessary hire external security experts to diagnose the underlying causes of the anomalous traffic.

d) Packet sampling

To make sense of the enormous amounts data flowing through a network, many leading providers use a technique called packet sampling. This technique involves developing rich views of traffic flow from samples of network traffic captured by routers. By reducing the amount of data that needs to be inspected, packet sampling allows operators of large networks to analyze traffic, even as the size and speed of modern networks increases.

Baseline Practices: Providers should at least sample packets at pseudorandom[†], giving packets a chance of being selected for inspection. This sampling may be performed on a content-neutral basis.

Advanced Capabilities: Providers can make use of more complex sampling techniques that weigh probability and adapt responsively to traffic changes. Providers may inspect for specific content associated with malware threats.

e) Honeypots and data level decoys

In addition to network level solutions described above, providers may make use of data level decoys such as honeypots to “bait” attackers. A honeypot is typically data or a system within a network that appears to be of value to malicious actors, who are then blocked or monitored when they attempt to access it. It is worth noting that honeypots and other decoys can be deployed by third parties, and providers may work with such entities to discover potential criminal activity or other cyber-attacks. Due to their usefulness in discovering criminal acitivity, honeypots are used in law enforcement sting operations.

Baseline Practices: Providers can deploy a low interaction honeypot, which has limited features and information-gathering capabilities but is low-risk because no actual intrusion takes place. The honeypot simulates a successful intrusion to fool attackers and collect information about them.

Advanced Capabilities: Providers can learn more about attackers by deploying a high interaction honeypot. Under this scenario, an attacker interacts with the provider’s actual system rather than an imitation, often exposing previously unknown attack vectors. Due to increased exposure to attacks, high interaction honeypots are inherently riskier, but also more revealing of attackers’ methods.

[†] *“Pseudorandom” numbers or processes have similarly unpredictable charcteristics to truly random numbers or processes, but aren’t actually mathematically random or unpredictable. In systems without means to generate true randomness, pseudorandomness is used.*

2. MITIGATE AGAINST DISTRIBUTED THREATS

Given detection of malicious traffic and potential threats, infrastructure providers can also apply a variety of mitigation methods, described below, to address these challenges.

Summary of Baseline Mitigation Practices: Providers should use ingress filtering — that is, apply a filter that can limit the rate of inbound traffic. Providers should also make a reasonable effort to shape traffic on their networks and use blackholing and sinkholing as network management tools.

Summary of Advanced Mitigation Capabilities: Companies with access to greater resources may use egress filtering in addition to ingress filtering, thereby limiting the rate of both outbound and inbound traffic. They may use access control lists (ACLs) to reduce attack vectors. Companies may take steps to minimize service disruptions when shaping traffic, for example by deploying selective black holes. They may use technologies such as BGP flowspec to increase traffic management options. They are able to work in partnership with government and industry to take down malicious botnets. They may also offer commercial services such as scrubbing traffic and DDoS protection.

a) Filtering

One of the complications when mitigating botnets is that malicious actors use IP-spoofing to make bad traffic appear to come from somewhere other than its actual place of origin.[44] By filtering out bad traffic as it enters the provider's network (i.e. ingress filtering, BCP38 and BCP84)[45], providers can reduce the effectiveness of spoofing and therefore make DDoS attacks more difficult to carry out. Due to the readily observable benefits of this practice, the Internet Engineering Task Force (IETF) has recognized ingress filtering as a best practice.[46] It is worth noting that ingress filtering works better at network ingress points such as customer premises, whereas it is much more difficult at network exchange points.

> **By filtering out bad traffic as it enters the provider's network, providers can reduce the effectiveness of spoofing and therefore make DDoS attacks more difficult to carry out.**

Moreover, while providers are often well-situated to filter malicious traffic, techniques such as BCP38 should be employed by any entity that is operating its own IP address space, including enterprises. Providers such as ISPs allocate many IP addresses to their clients who in turn may operate their own filtering capabilities and also need to follow BCP38.

Additionally, by deploying filters at the edge of their networks, providers can monitor the traffic coming out of, or egressing from, their corners of the ecosystem and reduce harm to other parties. Egress filtering is not a replacement for ingress filtering but rather a complementary solution. A combination of ingress and egress filtering is the best way for providers to increase resilience.[47]

Finally, in a network setting, ACLs are used to identify traffic flows based on parameters such as its source and destination, IP protocol, ports, EtherType, and other characteristics. A common example is that traffic from a lower security interface cannot access a higher security interface.[48] In some contexts, ACLs may be configured to account for the access privileges of individual users to further limit the attack vectors by which malware can infiltrate a network.

Baseline Practices: Providers should filter inbound traffic (ingress filtering) at network ingress points to reduce the amount of malicious traffic that enters their networks. The filter should be able to limit the rate of inbound traffic in the event of an attack that could overwhelm network resources.

Advanced Capabilities: Ideally, providers should filter outbound traffic (egress filtering) in addition to inbound traffic, and they should be able to limit the rate of traffic regardless of whether it is outbound or inbound. This hybrid solution provides a greater amount of protection and makes providers responsible neighbors to others in the ecosystem. Additionally, providers can use ACLs to reduce attack vectors.

b) Traffic shaping

When potentially malicious traffic is identified, providers can securely manage traffic either by using techniques that will typically result in the traffic being dropped or by delaying traffic when the data rate is anomalously high. Both of these techniques can be useful in specific circumstances and may be part of a comprehensive traffic management strategy.[49]

Baseline Practices: Providers should make a reasonable effort to shape traffic on their networks. At a minimum, providers should be able to deploy a “black hole” that prevents traffic from reaching a target. Efforts should be made to reduce disruptions to legitimate services by redirecting traffic or dropping traffic only within defined geographic regions.

Advanced Capabilities: Providers with more resources can shape traffic without causing as many disruptions to legitimate traffic. For example, commercial scrubbing centers can clean-up traffic by filtering out the malicious elements and sending legitimate traffic to its destination. Small providers may form partnerships with large providers to offer these services to their customers.

c) Blackholing

Blackholing is a technique that drops all traffic headed toward a specific online destination. A common version of this technique is remotely triggered destination based blackholing (RTDBH) in which upstream networks, which are typically closest to the attack source, drop the malicious traffic before it reaches a potential victim.

Although blackholing is effective at preventing malicious traffic from reaching its destination, an obvious drawback is that legitimate traffic cannot reach the destination either, which may be the explicit goal of malicious actors. To minimize this problem, providers may employ a technique known as selective blackholing, which drops traffic from chosen geographic regions (such as a country or continent) while allowing traffic from other regions to reach its destination.

Baseline Practices: Providers should make use of blackholing to protect their networks. While ideally providers should minimize disruptions to legitimate traffic, they should at least deploy the basic RTDBH in circumstances where more granular tools are not available or would not work as well.

Advanced Capabilities: Providers can improve the effectiveness of blackholing by leveraging partnerships with other providers both for sensors and filtering points of presence. Moreover, providers can deploy selective black holes that minimize disruptions to legitimate traffic by targeting a specific geographic region.

d) Sinkholing

Sinkholing is a technique where traffic within a particular IP-range is sent to a designated server (the "sinkhole") whereas traffic outside that IP-range continues as normal. The purpose of sinkholing is to capture botnets for both research and mitigation purposes.[50] Sinkholing is often accomplished through policy routing or other routing methods, which trap the malware that makes up a botnet in the sinkhole, where it can be studied by law enforcement and researchers. When malware caught in a sinkhole tries to communicate with command-and-control servers, security experts can track the IP addresses of machines the malware feeds information to, thus gaining insight into criminal activities. Providers can also completely sever communications between the malware and the command-and-control servers. Sinkholes are essential to large-scale takedowns of botnets, which use hundreds of thousands of internet-enabled systems in multiple countries throughout the world.

Baseline Practices: Providers should use sinkholing as a network management tool to redirect inbound malicious traffic and to collect information about threats to a provider's network for analysis or information-sharing.

Advanced Capabilities: Industry leaders can use sinkholes to disrupt and gather intelligence on ecosystem-wide threats in partnership with other providers and law enforcement. Providers can also assist international law enforcement operations by coordinating effectively with authorities and stakeholders across numerous jurisdictions.

e) Scrubbing

Scrubbing solutions are typically implemented by dedicated scrubbing centers, which analyze network traffic and cleanse it of malicious traffic, including DDoS. Because scrubbing is resource-intensive compared to other solutions, several large providers offer scrubbing as a commercial service. By redirecting traffic to the centers instead of dropping it, scrubbing allows legitimate traffic to reach its destination with a high degree of success. This makes scrubbing a preferable alternative to blackholing and sinkholing for many enterprises.

Advanced Capabilities: Scrubbing centers can add an important layer of protection to a provider or customer's defenses by filtering many types of attacks, not limited merely to volumetric flood attacks. For example, the centers may integrate technology that protects against SSL (encrypted links) based attacks.

f) BGP flowspec

Border Gateway Protocol (BGP) flow specification (flowspec) is a dynamic technology that enables providers to rapidly deploy a variety of different mitigation options, thereby allowing experts to make judgment calls on a situational basis. Unlike routers that only support blackholing, flowspec routers allow additional options such as sinkholing traffic so it can be studied by experts or, alternatively, shaping traffic and allowing it to proceed at a defined rate.[51]

Advanced Capabilities: Providers can use BGP flowspec to develop custom instructions for border routers instead of traditional one-size-fits all solutions. With BGP flowspec, routers can be instructed to either drop traffic, reroute the traffic, or limit the rate of traffic under appropriate validation of the flowspec originator.

3. COORDINATE WITH CUSTOMERS AND PEERS

Remediating botnets or other distributed threats may require providers to notify their customers or peers about a development to secure their cooperation. Obviously, the effectiveness of user-notifications hinges largely on the user. A study commissioned by M3AAWG found that telephone calls and postal mail are the most effective ways to get in contact with users.[52] Other available methods, which can and should be used, include email and webpage notices. Another method of contacting users is the "walled garden" — this approach limits user access to online services until they take specific steps determined by their provider. In some countries, approaches of this later kind raise legal or public policy concerns.[53] Peers can be notified with many of the same methods as customers. The notifications will be more effective if there is an established relationship. It is useful for providers to build familiarity with key players in their industries so that introductions do not have to be made for the first time during an emergency.

Baseline Practices: Providers should notify customers or peers who violate the acceptable use policy or engage in nefarious activities. If traffic from a customer or peer is blocked, provide both (1) a text or phone message *and* (2) email/user account webpage notice. The customer or peer should be provided with clear instructions on how to contact the provider via communications channels that are not being blocked.

Advanced Capabilities: Providers with trained staff and dedicated resources can greatly reduce the false positive rate so that customers rarely experience interruption when using services in a legitimate manner.

4. ADDRESS DOMAIN SEIZURE AND TAKEDOWN

Law enforcement has specific tools available that have been used in recent years to successfully mitigate malicious botnets and criminal actors with some success. Where good evidence exists that a criminal network is using particular domains to carry out their nefarious purposes (e.g., botnet attacks), a provider may work in cooperation with — and usually at the mandatory direction of — law enforcement to take down the domains, in accordance with relevant laws. Law enforcement action that leads to real-world consequences for malicious actors is the only solution that deals with the cause of botnets and DDoS attacks, rather than the symptoms. Law enforcement action of this kind is resource-intensive and often requires extensive forensic analysis. Large-scale domain seizures may also require international coordinated efforts.[54] For example, in 2016, providers worked with government officials from more than 30 countries to take down the Avalanche botnet and seize control of more than 800,000 domains scattered throughout the global internet and communications ecosystem.[55]

Baseline Practices: Providers should maintain an easy-to-find list of points of contact for law enforcement and security researchers. Providers should also have a well-defined policy describing how they can and cannot support law enforcement efforts.

Advanced Capabilities: Generally, industry leaders will have more procedures and technologies with which to support law enforcement. They will also have defined policies and legal positions on specific law enforcement tactics. They may conduct global risk assessment to account for global legal requirements. In addition to cooperating with law enforcement, providers may have processes for collaborating with competitors during exceptional events.

B. SOFTWARE DEVELOPMENT

Software is an increasingly ubiquitous element of every other component of the ecosystem addressed in this Guide. As discussed throughout this Guide, there are a wide variety of complex development processes and interdependencies that drive software innovation and improvement in the major systemic users of software highlighted in the Guide: Infrastructure, Devices and Device Systems, Systems Installers, and Enterprises. Accordingly, this section does not seek to capture the various baseline security practices and advanced capabilities that are pertinent to specialized software development in each part of the ecosystem. Instead, it aims to underscore the vital importance of secure software throughout and in all parts of that ecosystem. When not addressed specifically elsewhere in this Guide, software development should generally consist of these practices.

Baseline Practices and Advanced Capabilities for Software:

1. SECURE-BY-DESIGN DEVELOPMENT PRACTICES

Software and applications are increasingly integrated into our commercial and infrastructure processes and products to improve efficiencies. But this makes them a prime target for hackers. The global economy, critical infrastructure and government operations have increased their dependence on software.

Organizations that follow best practices make security an element of quality, conducting a range of secure development practices, including developer training, static application security scanning, threat modeling, dynamic application security testing, and manual penetration testing throughout the development lifecycle on a risk management basis. Resources to help developers adopt these best practices are publicly available. For instance, SAFECode (the Software Assurance Forum for Excellence in Code), a leading organization dedicated to promoting software assurance, publishes secure software development training resources available for free to the public, including the *Fundamental Practices for Secure Software Development.*[56]

Baseline Practices: Secure-by-design development should include the following at a minimum:

- ***Strong encryption of data at rest and in transit:*** Encryption inhibits the visibility of data in the event that it is stolen or improperly accessed. Whether the data is resting (i.e. stored) or in transit, encryption is an essential tool to protect information. While there are different encryption options suited to the needs of specific organizations and products, the encryption should generally use a strong algorithm that cannot be broken easily in the context of its particular use case. The strength of an algorithm may vary contextually, depending on factors such as the type of attack at issue and the need for certain kinds of services to function properly. For example, strong encryption may prevent most firewalls and other security packet inspection services from working.
- ***Security by default:*** The default configuration settings of software should place a high emphasis on security. The settings should have to be deliberately changed in order for the software to lower its defenses to allow for more options. This principle reduces the attack vectors that malicious actors can exploit significantly.
- ***Patchability and design for updating:*** Software should be designed with the expectation that patches and updates will be necessary to protect against malicious actors' constantly evolving and increasingly sophisticated attacks. Patches and updates should be deliverable with minimal manual intervention in a reasonably quick and secure manner to systems with the software installed.
- ***Principle of least privilege:*** By limiting user and application access to only the essential privileges needed to perform necessary tasks, software developers can reduce the attack surface of a product. Applying the principle of least privilege in the design phase reduces the chance that a malicious actor or compromised service will gain administrative access and control over a system.
- ***Software composition analysis:*** The purpose of this analysis is to create an inventory of open source and other third-party components in the product. In doing so, software developers can maintain awareness of components they did not develop themselves in case problems arise, even if they cannot guarantee the security of third-party and open source components. Having an inventory of what components are used in products and applications can also help development organizations track and identify associated known vulnerabilities.
- ***Software security awareness and education:*** Awareness-raising should extend to all personnel who are part of the software development process, including developers, product managers and others. Cost-effective educational opportunities or training exercises should be made available.

Advanced Capabilities: Leading secure-by-design practices include the following:

- ***Dynamic application security testing (DAST):*** This advanced technology uses penetration testing (a simulated attack) to discover vulnerabilities while an application is running. This kind of testing can be especially useful in the IoT context. However, it requires manageable configuration options and the ability to hire highly skilled specialists.

- ***Static application security testing (SAST):*** With this advanced technology, developers can scan source code or binaries and identify vulnerabilities. It is limited to supported languages and platforms. For many products in the IoT space, this might not be an option. However, careful peer code review of especially sensitive components may be used to increase security.
- ***Threat modeling and analysis of risks to architecture:*** Companies that work with governments or whose operations are highly sensitive may hire teams of experts to determine how malicious actors would hypothetically create or exploit vulnerabilities in a system to achieve nefarious ends. A threat model may consider many types of risks, including those involving automated, distributed attacks.
- ***Security-focused toolchains:*** Developers may make use of security-focused toolchains to create new software. A toolchain is a collection of software or hardware tools that facilitate software development. When toolchains prioritize security, coding errors are less frequent and providers can enforce quality controls. Companies may integrate new vulnerabilities and lessons learned into development tools.
- ***Secure third-party and open source components:*** Leading companies will ensure third-party components and open source libraries being used are free of known vulnerabilities.
- Additionally, companies may provide attestation to customers about elements of secure software development process and seek certification of alignment with international standards.

2. SECURITY VULNERABILITY MANAGEMENT

Different companies throughout the world have different policies with regard to when and for how long security patches are available to customers after a product ships in order to remediate newly discovered vulnerabilities. While major product manufacturers tend to release patches for their products more regularly, smaller manufacturers are generally less likely to devote sufficient resources to developing and making available security patches.[57]

Baseline Practices: Providers should prioritize critical vulnerabilities in mission critical applications.

Advanced Capabilities: More advanced providers can fix nearly all known vulnerabilities, especially those prioritized during risk assessment. They have the ability to provide security assurance to those purchasing software from their company or interacting with their company through applications.

3. TRANSPARENCY OF SECURE DEVELOPMENT PROCESSES

Each of the above practices plays an important role in the development of secure software and hardware. Software development organizations and the private sector have initiated the development of market-based assessments of secure development processes.[58] However, a framework developed in partnership between government and industry stakeholders could help standardize terminology and processes, building stronger market confidence. NIST is currently partnering with SAFECode and other stakeholders to develop a special publication on secure software development processes and practices. NTIA is convening a multistakeholder process to explore how organizations can communicate information about third-party software components and offer greater transparency.[59]

Baseline Practices: Provide attestation of security posture to companies purchasing software.

Advanced Capabilities: Provide security assurance to those purchasing software from the company and interacting with the company through applications.

C. DEVICES AND DEVICE SYSTEMS

An individual connected device (or “endpoint device”) may itself consist of multiple components, including hardware modules, chips, software, sensors or other operating components. Hundreds of thousands of companies and millions of developers potentially contribute to the billions of individual devices deployed throughout the world. Beyond the individual device itself are multiple additional layers of connectivity that constitute a highly dynamic new market — including for security innovation. To put it simply, connected devices are no longer simply individual devices. Instead, with this complexity in mind, this Guide addresses Device Systems: the union of a connected endpoint device — that is, one “thing” in the Internet of Things — and its associated support elements elsewhere in the internet, including apps and cloud services.[60]

Baseline Practices and Advanced Capabilities for Devices and Device Systems

1. SECURE-BY-DESIGN DEVELOPMENT PRACTICES

Security is best and most efficient if it is part of the early development process and is included as a key factor throughout that process. Certain categories of best practices have become commonly accepted as necessary tools for ensuring that the end product has essential confidentiality, integrity, and availability.[61] Botnets take advantage of weaknesses in the implementation of devices and systems, so it is only appropriate to include security planning early on and at all stages of product development to avoid such weaknesses.

a) Secure Development Lifecycle Process

Baseline Practices: A secure development lifecycle (SDL) process should be in place. In the SDL process, each development phase has security activities that can be done manually or automatically.[62]

Advanced Capabilities: After establishing a secure development lifecycle process, the advanced company is measuring and growing process capabilities. Measuring SDL capabilities is part of the BSIMM project (Building Security In — Maturity Model[63]); the BSIMM materials are open source and can be a resource for this effort.

b) Elements of Secure Design

This section lists practices that are at the developer level in product design.

(1) Means to protect data at rest and in transit

This category is primarily about protecting stored data on the device and encrypting data communications. Implementing such protections may involve decisions regarding, e.g., secure hardware elements, secure boot process, etc.; see also Advanced Capabilities: Roots of Trust.

Baseline Practices: Data communications should be encrypted. Sensitive data should be stored encrypted. Regardless of whatever protocols are in use, if authentication is available, it should be used. In general, the security mechanisms available in whatever system is used should be employed. Cryptographic techniques used should avoid deprecated methods.

Advanced Capabilities: The latest versions of protocols and security mechanisms should be used. Secure memory can be used in lieu of encryption for stored information. Encryption key methods comporting with NIST FIPS 140-2 or ISO/IEC 24759 should be used.[64]

(2) Means to restrict unauthorized access

Baseline Practices: IoT products typically require local or remote administrative services. During product development and manufacturing there may be requirements for other kinds of low-level access to memory, processor, peripherals, or control flow that are not required or available to the end user of the device. These additional capabilities must be carefully protected.

Typical steps at this level include: Unique “admin” credentials per device or a first-boot requirement to change passwords; rate-limiting techniques to prevent brute-force password guessing; securing or disabling developer-level ports and services prior to product shipment; removing unused or insecure local and remote administrative services such as telnet.

Advanced Capabilities: Multi-factor authentication user access control should be supported.

In addition, endpoint device and router developers should consider new and emerging standards that specifically assist in preventing unauthorized access and use by botnets. For example, the IETF Manufacturer Usage Descriptor (Proposed Recommendation) or “MUD”[65] may be appropriate for many use cases. MUD is “an embedded software standard defined by the IETF that allows IoT Device makers to advertise device specifications, including the intended communication patterns for their device when it connects to the network.”[66] When both the device and the router adhere to MUD requirements, the router has a mechanism for limiting a device to the purposes intended by the manufacturer. Activities outside those purposes — such as participating in a massive DDoS attack — can be identified and blocked by the local router. Additional standards such as IEEE 802.1AR[67] and the Device Identifier Composition Engine (DICE)[68] architecture can improve the security of the IoT device and its MUD components.

(3) Use of obfuscation

Baseline Practices: Device manufacturers should not rely solely on use of obfuscation to secure secrets (e.g., device keys, sensitive data), but obfuscation may be used to increase the difficulty of an attacker to locate the secret. Still, the secret should be protected by other means such as access control and encryption.

Advanced Capabilities: Implementation of Baseline as well.

(4) User input validation and system output encoding

Baseline Practices: Any input received from outside the system must be managed so that an outside adversary cannot take advantage of unintended consequences. Input should be validated for length, character type, and acceptable values or ranges; see also whitelist filtering. Output from one subsystem to another or to another site should also be filtered; see "character canonicalization."

Advanced Capabilities: Implementation of Baseline as well.

(5) Cryptography commensurate with the needs of the product

Baseline Practices: Cryptographic methods are required to ensure data integrity and confidentiality, rights authentication and non-repudiation of requests. This cryptography should be chosen to match the assessed risk but should use open, peer-reviewed methods and algorithms. Where feasible, cryptographic methods are updateable.

Advanced Capabilities: Strong, proven, updateable cryptography using open, peer-reviewed methods and algorithms. Ensure cryptography has the ability to support post-quantum resistant key lengths for symmetric encryption.

2. ROOTS OF TRUST

Various types of attacks rely on imitating another entity. For example, a trusted source for new software for a device is generally the original hardware manufacturer. Installation of software corrupted with malware is obviously something to prevent. This begs the question of how to tell the difference.

The solution is to have a system of trust. A trust chain is a linkage of hardware and software elements in which each element is validated as it is added to the chain. At the beginning of the chain is a root of trust, which is provided by an authoritative entity. Validation is done cryptographically, using digital signatures. Because the first element ties back to a trusted authority, each element that is cryptographically validated by the chain can also be trusted.

When the system receives a signed software update, it can check the digital signature. Because the system itself is rooted in the trust of the original authoritative entity, after the software update is validated, the software can be trusted.

a) Hardware-Rooted Security

Baseline Practices: Consider how hardware-rooted security fits into the secure development lifecycles of current and future products.

Advanced Capabilities: Hardware-rooted security is utilized where technically feasible.

3. PRODUCT LIFECYCLE MANAGEMENT INCLUDING END-OF-LIFE

Product Lifecycle Management refers to actively managing a product from conception through design, manufacturing, support and end-of-life. End-of-Life Management refers to having a defined policy as to what should be done when the product has reached a defined endpoint in its lifecycle, including the end of a defined support term, or end of functionality, or end of a calendar period, etc.

Baseline Practices: Device manufacturers may provide notice to the consumer about security support policy and how the device is supported with updates during and what to expect after the support period. Where possible, the device should support network asset management by enabling the ability to identify and audit the device logically and physically and with proper access control.

After the support period, consumers should have the ability to, and be informed about, how to “decommission” the device. Decommissioning should allow a consumer to return the product to factory defaults and remove any Personally Identifiable Information (PII). This capability covers a variety of scenarios such as the sale, abandonment, or recycling of the product, including selling a property with IoT devices installed.

Providers should create a security vulnerability policy and process to identify, mitigate, and where appropriate disclose known security vulnerabilities in their products.

Advanced Capabilities: A plan for secure updates with anti-rollback protection and proper access control throughout a defined security support period, where technically feasible.[69]

4. SECURITY-FOCUSED TOOLCHAIN USE

Security-Focused Toolchains are collections of software or hardware that not only enable development, production, and management of products, but also have been designed to enhance the security of the end product.

Baseline Practices: Tools that are able to check if the implementation is following secure coding guidelines and to search for a subset of known Common Vulnerabilities and Exposures (CVEs) in the open source software should be used.

Advanced Capabilities: Tools such as fuzzing, symbolic execution, sandboxing, static and dynamic analysis, and memory-safe languages are used to find and mitigate vulnerabilities.

D. HOME AND SMALL BUSINESS SYSTEMS INSTALLATION

Homes and small businesses benefit from connected devices in several categories. Heating, ventilation, and air conditioning (HVAC) systems are connected for smart features and remote access by the occupant. Security systems include cameras, locks, and alarm systems that can all be managed via the internet. Entertainment systems benefit from central controls so that complex audio and video configurations can be managed with ease. There is tremendous diversity of manufacturers and systems in these categories. These systems can be installed by do-it-yourself home and business owners, or by professionals: integrators, alarm contractors, and others.

Ideally, every device and system entering a home, office, retail, medical, or industrial environment will be secured by best practices in the entire lifecycle of the device. This lifecycle includes installation and configuration of the device. A good installation will achieve the “best available security” from the manufactured product. In this section are baseline practices and advanced capabilities for achieving that best available security from the most common device types.

The material below draws heavily from *The Connected Home Security System*.[70]

Baseline Practices and Advanced Capabilities for Home and Small Business Systems Installation

1. AUTHENTICATION AND CREDENTIAL MANAGEMENT

Installations can benefit from Password Management Systems, which are encrypted storage for passwords. These systems take the burden away from users of remembering and managing passwords and putting the passwords in a secure place.

Baseline Practices: If a password is not unique to the device, the installer should change to a strong password. (See [1], “Passwords”). Different passwords must be used for all devices and systems. The installation should use a trusted password management system.

Advanced Capabilities: Multi-factor authentication user access control is used.

2. NETWORK CONFIGURATION

Network Configuration refers to the physical and logical layout and connections and settings of network components.

a) General

Baseline Practices: Systems (desktops, laptops, etc.) should have up-to-date anti-virus and anti-malware tools installed and running. No systems with administrative privileges should be running unless specifically required.

b) Firewall, Access Point, and Router Configuration

Baseline Practices: UPnP should be disabled on the WAN side (internet facing side) unless required for a legitimate purpose (e.g., peer-to-peer gaming). Adequate DHCP space should be allotted for expected usage but not exceed expected usage. A firewall should be enabled with only required ports unblocked. Port forwarding should be disabled except for specific applications where it is required.

Advanced Capabilities: Networks should be monitored, use non-standard port values on applications, and have port forwarding only selectively enabled for specific applications in conjunction with firewall protections. Although a sophisticated attacker can overcome it, MAC address filtering should still be used.

c) Physical and Logical Structure

Baseline Practices: Network access should be limited from outside the physical structure of the client site in terms of wireless power and physical wiring placement. Segments should be separated according to purpose and use separate physical or logical networks, using options such as separate radio channels, cabling, separate access points, or gateways.

Advanced Capabilities: Segments should additionally be separated for different purposes using VLANs or VPNs. A port scanning tool can be used to monitor the private network.

3. NETWORK HARDWARE MANAGEMENT

Network Hardware Management refers to the ongoing process of keeping network devices properly identified and configured.

a) Modems and Routers, Network Management Devices

Baseline Practices: Networking devices should have a process or means for regularly updating firmware.

Advanced Capabilities: For ISP-provided modem/router/AP systems, a separate aftermarket router/AP can be added to handle LAN traffic for local control over software updates.

b) Network Protocols

Network Protocols are the multilevel languages devices used to communicate on networks, such as TCP, UDP, IP, RTP, etc.

Baseline Practices: Deprecated protocols should not be used. In particular, do not use or allow to be negotiated SSL (any version), or TLS 1.0 or 1.1.

Advanced Capabilities: Configure for the latest protocols where appropriate.

c) Wireless Links

Wireless Links are radio-based network connections between devices. These links may be one way, bidirectional, or use a network topology among multiple devices.

(1) Bluetooth

Baseline Practices: Available security features should be enabled. “Non-discoverable” options should be used where available. No sensitive information should be exposed in Bluetooth low energy (BLE) beacon signals.

(2) NFC

Baseline Practices: NFC readers should not be situated or mounted to allow for easy “sniffing” or for easy tampering.

(3) Wi-Fi

Baseline Practices: In addition to the Baseline network configuration practices mentioned in other sections, up-to-date Wi-Fi encryption options should be used, such as WPA2-Personal with AES (preferred) or WPA2-Personal with TKIP. WPS should be disabled. Neither default nor broadcast SSIDs should be used.

A “guest network” option is available on many Access Points; this should be enabled and made available for higher-risk users such as visitors or temporary residents/workers. If available, 802.11aw Management Frame protection should be enabled. Ensure the Access Point configuration access is protected with a strong password under the best practices described elsewhere in this document. Enable port filtering where appropriate. Choose an Access Point/Router with updatable firmware.

(4) Z-WAVE

Baseline Practices: Basic security involves unique Home IDs, password-protected administrative functions, and use of AES-128 enabled devices where available.

Advanced Capabilities: To increase security, RF power can meet the distance requirements and exclusively AES-128 enabled devices can be used.

(5) Zigbee

Baseline Practices: The only device connected to the internet should be the ZigBee gateway and there should be a firewall protecting it.

Advanced Capabilities: Internet traffic can be filtered when entering and leaving the ZigBee network by address (source and destination) and port number. Optional 802.15.4 security features can be enabled at the 802.15.4 level and at the network plus application level, where available.

(6) Remote Device Access Control

This category involves all kinds of remote access control of normal device functions such as security camera video, HVAC temperature control, vehicle subsystems such as remote start or door unlock, etc.

Baseline Practices: Alerts for device failure or tampering should be enabled when available. All remote access should be behind an IP restricted firewall, allowing only white-listed IP addresses and subnets to access the device, regardless of port. If remote access from outside the firewall is a required feature, VPNs and non-standard internet ports should be used for remote access.

4. SECURITY MAINTENANCE

Baseline Practices: Where possible, breach attempts on the network or other attempts on the installation should be tracked and reviewed for action. Breach attempts should be correlated to identify commonly attacked individuals or targets within the network. Network configuration should be documented, connected devices should be enumerated, and a security maintenance plan should be clearly defined.

E. ENTERPRISES

As major owners and users of networked devices and systems, including an exponentially increasing number of IoT device systems, enterprises of all kinds — government, private sector, academic, non-profit — have a critical role to play in securing the digital ecosystem.[71] While enterprises often are the victims of automated, distributed attacks as well as data exfiltration attempts, their vast systems also can be hijacked to increase the impact of DDoS and other distributed attacks on others. Accordingly, enterprises are collectively among the important stakeholders that share responsibility for adequately securing their networks and systems in order to help secure the broader digital ecosystem.

The millions of private sector and government enterprises worldwide differ considerably in terms of their technical knowledge and skills, access to resources, and incentives to adopt baseline security practices. Larger enterprises, for instance, often have a Chief Information Officer and a Chief Information Security Officer, each charged in part with securing the organization’s networked systems and devices, including any IoT systems. Smaller enterprises may not have the resources for dedicated IT and information security personnel and instead rely on off-the-shelf solutions.

Organizations increasingly are developing and offering tools to help enterprises, both small and large, secure their networks and systems. Perhaps most relevant to the Anti-Botnet Guide is the effort by the Cybersecurity Coalition to develop and advance Profiles for DDoS and Botnet Prevention and Mitigation Profile under the Cybersecurity Framework,[72] intended to aid enterprises and other organizations in addressing and mitigating DDoS and other automated, distributed attacks.

Enterprises of all sizes also can take their own proactive steps to mitigate ecosystem risk through, for example, implementing appropriate identity and access management techniques and discontinuing the use of legacy and pirated products and software that do not receive updates, among other things. Steps like these can help enterprises protect sensitive data and intellectual property on their networks, in addition to helping to protect the ecosystem at large by reducing the attack surface for DDoS and other distributed attacks.

Of course, the suppliers and providers that developed this Guide are ourselves large global enterprises. Further, we provide high-end solutions to secure enterprise networks and mitigate against DDoS attacks and other automated, distributed threats. The “supply” side of this market is robust and growing; further development of the “demand” side of this market in terms of enterprises of all sizes requesting and negotiating for these services will bring further innovation, sophistication, and cost efficiencies in these services.

Baseline Practices and Advanced Capabilities for Enterprises

1. SECURE UPDATES

While product manufacturers are responsible for creating secure updates, those updates generally do not install themselves without permission or other action by the user. The level of control organizations may need over updates varies considerably depending on the type of customer. A large enterprise or government agency with qualified staff, for example, can reasonably determine which kinds of security updates are appropriate and when to implement them. On the other hand, regular home users may benefit most from automatic updates.[73]

Baseline Practices: Enterprises should install updates as soon as they become available. Generally, automatic updates are preferable.

Advanced Capabilities: Enterprises with qualified technical staff can make informed determinations about the implementation of security updates.

> **Enterprises are collectively among the important stakeholders that share responsibility for adequately securing their networks and systems in order to help secure the broader digital ecosystem.**

2. REAL-TIME INFORMATION SHARING

Enterprises with large networks or highly sensitive networks (e.g., large enterprises and government agencies) can share critical threat information with other relevant stakeholders and ecosystem participants. These efforts have improved significantly in recent years and constitute a big step forward toward combating the threat of botnets and other automated, distributed threats.[74]

Baseline Practices: Enterprises should be prepared to receive and act responsively and responsibly upon cyber threat information provided by information sharing activities even when not yet committed to actively share information. Examples include information from government and law enforcement information sharing activities, various CERTs, industry groups, network providers, RFC2142 addresses, and updates and alerts from vendors and other sources.

Enterprises should subscribe to multiple threat intelligence feeds or services to utilize in conjunction with security information and event management (SIEM) correlation/automation efforts. Enterprises should have processes in place to share threat information gained internally or externally with internal shareholders in a timely and actionable manner. Enterprises should maintain contact with sharing communities and be aware of the processes and safeguards to properly report/share cyber security incidents within their region and industry. Enterprises should conduct internal threat intelligence sharing on an ongoing basis. Indicators of compromise (IOCs) and notable threats should be shared on a regular cadence.

Advanced Capabilities: Advanced enterprises should be committed to enhancing the cyber threat information sharing community through the responsible and timely sharing of desensitized cyber threat information with the various appropriate sharing communities (government, industry, etc.). Advanced enterprises should ensure that they have sufficient capabilities to detect, analyze, and capture cyber threat information in formats that are conducive to sharing activities. Advanced enterprises should actively participate in the governance and enhancement of cyber threat information sharing communities appropriate to their region and industry. Advanced enterprises should seek to continuously improve their capabilities in detection, analysis, response, and sharing.

3. NETWORK ARCHITECTURES THAT SECURELY MANAGE TRAFFIC FLOWS

Enterprises can exercise control over the design of their network architectures to limit the flow of malicious traffic during a DDoS attack carried out using botnets or other means.[75] A network architecture designed with security as an explicit goal can complement other precautionary measures, such as anti-DDoS services offered by infrastructure providers and other ecosystem participants. Application Programming Interfaces (APIs) manage the connections between applications, devices, and back-end data systems. Broadly speaking, APIs make it possible for enterprises to open their back-end data and functionality for reuse in new application services. Deploying security at the perimeter, through an API Gateway, can help enterprises stop threats before they penetrate the enterprise, allowing them to provide access to enterprise data for application developers while maintaining strong security.

Baseline Practices: Enterprises should obtain intranet defense against DDoS by consuming capabilities and services provided by network service providers. Enterprises should standardize the internet to intranet interconnect architecture, operational policy and processes, access and packet flow control configuration settings. Enterprises should implement a regime that ensures this architecture is correctly deployed and operated. In addition, enterprises should inspect all inbound and outbound data flows and email and block packets or emails with malware; block unauthorized network traffic into the intranet; and utilize industry standard DMZ architecture and operational practices.

Advanced Capabilities: Advanced enterprises may identify observable behaviors that indicate botnet flows, such as botnet C&C flows, fastflux DNS, and accessing suspicious URLs. Advanced enterprises may automatically block botnet flows and remediate the sources of the flows; remove internet accessible URL links from inbound emails; share and receive information that is used to identify botnet actors; and prevent improper DNS actions by both the DNS requester and the DNS server.

To increase resiliency against distributed attacks, advanced enterprises may make use of Application Programming Interface Gateways. Application Programming Interfaces (APIs) manage the connections between applications, devices and back-end data systems. Deploying security in a centralized architecture through an API Gateway can help organizations provide access to enterprise data for application developers while maintaining strong security.

4. ENHANCED DDOS RESILIENCE

Even with very successful customer awareness and educational outreach efforts, many customers will lack the technical expertise required to secure their own networks. Rather than ignoring the threat that botnets and other distributed attacks may pose, enterprises should purchase commercial DDoS protection suitable to their risk profile.[76] Commercial services may include off-premise protection or a combination of off-premise and on-premise protection that more robustly secures the enterprise against distributed attacks. When customers purchase commercial products and services, they substantially decrease the threat of botnets and other distributed attacks.

CSDE's members provide some of the highest-end commercial DDoS solutions on the market. Examples include home gateways with integrated security, Anycast services, and a variety of managed security services. Anycast services increase resilience to DDoS attacks by providing multiple routes for content delivery and balancing workloads across multiple network elements, which may be spread throughout the world. If a DDoS attack compromises certain parts of a network, traffic is rerouted automatically to another part. Managed security services include commercial scrubbing services.[77] Other commercial services include network-based firewalls, mobile device management systems, threat analysis and event detection, secure VPN connectivity to the cloud, web and application security, and email security.

Providers may offer filtering solutions tailored to the unique needs and risk profiles of their customers. Ideally, these solutions will integrate both off-premise and on-premise defenses. Commercial services may allow malicious traffic to be blocked closer to the attack source, creating an extra layer of security for customers.

Baseline Practices: Enterprises should have capable retained/contingency support available to them to effectively respond to cyber security incidents and maintain a reasonable level of security. Enterprises should select commercial providers whose products and services include appropriate security capabilities (i.e., ISPs and cloud/hosting providers who have DDoS protection capabilities, software with auto-update capabilities, etc.). Enterprises should have documented, tested plans for incident response, including DDoS and botnet response. Enterprises should select commercial providers who can provide automated or default-on response. Enterprises should regularly re-evaluate the effectiveness of the commercial providers.

Advanced Capabilities: Advanced enterprises should take a multi-layered approach to DDoS and botnet protection that includes well-supported on and off-premise capabilities. Advanced enterprises should proactively increase their staff's technical expertise, determine gaps in this expertise, and address these gaps with appropriate training, retained/contingency support, and additional staff. Advanced enterprises should consider commercial services and software that offer advanced capabilities such as machine learning and pattern analysis to enable higher quality results. Advanced enterprises should seek to continuously improve their capabilities by regularly re-evaluating the capabilities available in the marketplace.

5. IDENTITY AND ACCESS MANAGEMENT

Identities constitute the unifying control point across applications, devices, data, and users. Identity and access management tools authenticate individuals and services and govern the actions they are permitted to take. One of the most important areas of IT risk relates to privileged users, such as IT Administrators, CISOs, and other individuals with enhanced systems access. Whether inadvertent or malicious, improper actions by privileged users can have disastrous effects on IT operations and the overall security and privacy of organizational assets and information. Systems should be set up for administrators to only perform those actions that are essential for their role — enabling "least privileged access" for reduced risk. Threat analytics can provide insight on activity and work to prevent or flag anything unusual that indicates security risk.[78]

A recent development worth noting is the use of physical security keys instead of passwords or one-time codes. Since early 2017, when Google began requiring all of its employees — more than 85,000 in total — to use physical security keys, not a single employee's work-related account has been phished.[79]

> **When customers purchase commercial products and services, they substantially decrease the threat of botnets and other distributed attacks.**

Baseline Practices: The identity and access management practices of organizations should at least include the following:

- ***Authentication*** (including multi-factor and risk-based authentication) — a time of access operation that assures that the subject is in fact the real subject and not an impersonator;
- ***Authorization*** — a time of access operation that determines, given the current state, whether access should be granted;
- ***Access Governance*** — a process for helping business leaders define and refine policies for determining appropriate access;
- ***Accounting*** — a process for logging data about the activity of individual users who access system resources to analyze trends and identify suspicious behavior;
- ***Provisioning/Orchestration*** — a set of operations that happens at times of change facilitating the join/move/leave process and the coordination of change events between disparate connected resources; and
- ***Identity Repository*** — a persistent store for maintaining the current state and attribute values of subjects' profiles.

Enterprises should also adopt the practice of offboarding, which is the timely removal of identity from enterprise directory and revocation of identity and associated accesses, within 24 hours for privileged accesses and accesses to cloud resources.

To improve authentication, enterprises should use stronger and easier-to-remember passphrases instead of syntax rule-based passwords; check against a password dictionary; and use a password strength meter. Moreover, enterprises should make use of second or Multi-Factor Authentication (2FA/MFA) for privileged accesses, e.g., System Administrators. Organizations should use a centralized authentication service for web and SaaS applications with Single Sign-on which requires 2FA — step-up authentication — for devices that are not previously vetted and trusted. Moreover, enterprises should use FIDO U2F tokens to thwart phishing attacks or take other reasonable precautions to reduce the risk posed by phishing attacks.

Enterprises should adhere to the principle of least privileged access — access request based on roles via Role-Based Access Control (RBAC) and/or approvals, detection, and remediation of out-of-process, outlier, dormant, and Separation of Duties (SoD) violation accesses, and accesses governance via periodical revalidation of accesses (Continued Business Needs or CBN).

Enterprises should conduct privileged user monitoring and audit and Secure Information Event Management (SIEM). They should also have a credential/secret vault for service or application IDs — the IDs should not be stored in configuration files in plain-text.

Advanced Capabilities: Advanced enterprises may have more sophisticated methods of managing identity and access:

- ***Continuous authentication*** methods leverage behavioral and biometrics monitoring throughout a user session to determine if the session has been compromised.
- ***Risk-based authentication*** provides enterprises with a better understanding of the context around identity, such as through geo-location data or purchasing behavior. A system may recognize the identity, determine that traditional authentication is unnecessary, and allow access. Conversely, if the system detects anomalies, such as logging in from a foreign country in the middle of the night after having a few failed passwords, then this is a very high-risk operation and access will be denied absent additional authentication steps.
- ***Privileged Access Management*** solutions provide the visibility, monitoring and control needed for those users and accounts that have the "keys to the kingdom." It is essential that administrators be allowed to perform only those actions that are essential for their role — enabling "least privileged access" for reduced risk. This visibility provides insight on activity and works to prevent or flag anything unusual that indicates security risk.
- ***Adaptive authentication*** uses 2FA/MFA, with more complete and sophisticated risk calculation, above and beyond device fingerprinting, incorporating factors like intranet or internet, simultaneous access from multiple locations or geographies, logging-in at very odd hours, etc.
- ***Closed-loop identity*** governance integrates user activity monitoring and analytics on servers and inside applications with access management tools, e.g., revoke a privileged user's access if he/she is detected of accessing protected data on server or inside applications in an unauthorized manner.
- ***Smarter access*** governance can be achieved with analytics and AI, e.g., detecting and revoking dormant accesses — accesses that have not been used by their owners for a prolonged period, signaling potential lapses in access governance or offboarding.
- ***Detection of and safeguarding against hacking*** can be improved with integration of privilege access management and User and Entity Behavior Analytics (UEBA): malware dropped onto workstations via spear phishing using social network info and emails will behave differently and can indicate that a workstation and privileged credentials have been compromised.

IN THE U.S., ALMOST

1 in 5

PERSONAL COMPUTERS RUN PIRATED SOFTWARE

whereas

IN CHINA THE PERCENT OF PERSONAL COMPUTERS WITH PIRATED SOFTWARE **OFTEN EXCEEDS**

70%

6. MITIGATING ISSUES WITH OUT-OF-DATE AND PIRATED PRODUCTS

Enterprises should discontinue use of the legacy products for which manufacturer support has ended.[80] A closely related problem from a technical support standpoint is pirated software. In the U.S., almost one in five personal computers run pirated software, whereas in China the percent of personal computers with pirated software often exceeds 70%.[81] Of course, manufacturers do not normally patch pirated software, which means it remains vulnerable to known exploits.[82] Enterprises should avoid pirated software and decrease the total number of vulnerabilities in the global internet and communications ecosystem.

Baseline Practices: Enterprises should replace legitimate supported products before manufacturer support expires. Enterprises should always avoid pirated products. Such products are illegal in most countries and they are also major contributors to security vulnerabilities throughout the ecosystem.[83]

Advanced Capabilities: Advanced enterprises may have the latest supported products available with the most up-to-date security features and capabilities.

06 Next Steps and Conclusion

Publication of Version 1.0 of this Guide constitutes the first step of an unprecedented industry-led strategic campaign against botnets and other automated, distributed threats. The CSDE, USTelecom, ITI, and CTA urge stakeholders to implement the recommended practices to address the common challenges and turn the tide against bad actors.

As noted in the Introduction to the Guide, the digital economy has been an engine for commercial growth and quality-of-life improvements across the world. No single stakeholder — in the public or private sector — controls this system, so securely managing the opportunities presented by this growth is the imperative responsibility of every stakeholder in the ICT community.

To that end, we set forth these baseline practices and advanced capabilities for the consideration of all stakeholders. These are dynamic, flexible solutions that are informed by voluntary consensus standards and driven by powerful market forces, and they can be implemented by stakeholders throughout the global digital economy. This is the best answer to the systemic cybersecurity challenges we face.

With this imperative in mind, we plan to update, publish and promote a new version of this Guide on an annual basis, reflecting the latest developments and technological breakthroughs that will aid our companies and other companies throughout the world to drive observable and measureable security improvements — not only within their own networks and systems but also throughout the broader ecosystem.

More immediately, our next step in coming months is to promote this Guide with a broad spectrum of national and international stakeholders in the internet and communications ecosystem who are well-positioned both to promote the recommended practices and further constructive engagement. The shared responsibility assumed by these diverse stakeholders is the key to securing the future of our digital economy.

07 Contributing Organizations

About CSDE

The Council to Secure the Digital Economy (CSDE) brings together companies from across the information and communications technology (ICT) sector to combat increasingly sophisticated and emerging cyber threats through collaborative actions. Founding partners include Akamai, AT&T, CA Technologies, CenturyLink, Cisco, Ericsson, IBM, Intel, NTT, Oracle, Samsung, SAP, Telefonica and Verizon. CSDE is coordinated by USTelecom and the Information Technology Industry Council (ITI).

About USTelecom

USTelecom is the premier trade association representing service providers and suppliers for the telecom industry. Its diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives — all providing advanced communications service to both urban and rural markets.

About ITI

The Information Technology Industry Council (ITI) is the global voice of the tech sector. As the premier advocacy and policy organization for the world's leading innovation companies, ITI navigates the relationships between policymakers, companies, and non-governmental organizations, providing creative solutions that advance the development and use of technology around the world.

About the Consumer Technology Association

The Consumer Technology Association (CTA)™ is the trade association representing the $377 billion U.S. consumer technology industry, which supports more than 15 million U.S. jobs. More than 2,200 companies — 80 percent are small businesses and startups; others are among the world's best-known brands — enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development and the fostering of business and strategic relationships. CTA also owns and produces CES® — the world's gathering place for all who thrive on the business of consumer technologies. Profits from CES are reinvested into CTA's industry services.

08 Endnotes

1 Malicious actors are also commonly referred to as hackers, although not all hackers are malicious. Generally this document uses the terms interchangeably, with the assumption that context will indicate whether the referenced individual is a malicious actor or not. It should also be noted that this document focuses on malicious actors, so generally speaking, "hacker" in this document is a malicious actor

2 It is not practical to set requirements of all software types in the IoT ecosystem simultaneously. Devices and Device Systems, Enterprises and Infrastructure have specific requirements. This section applies to areas not covered elsewhere in the Guide.

3 An individual connected device (or "endpoint device") may itself consist of multiple components, including hardware modules, chips, software, sensors or other operating components. Hundreds of thousands of companies and millions of developers contribute to the development of the billions of devices deployed throughout the world. Beyond the individual device itself are multiple additional layers of connectivity that constitute a highly dynamic new market, including for security innovation. To put it simply, connected devices are no longer simply individual devices. With this complexity in mind, this Guide addresses Device Systems: the union of a connected endpoint device — one "thing" in the IoT — and its associated support elements elsewhere in the internet, including apps and cloud services.

4 Heating, ventilation, and air conditioning (HVAC) systems are connected for smart features and remote access by the occupant. Security systems include cameras, locks, and alarm systems managed via the internet. Entertainment systems benefit from central controls so that complex audio and video configurations can be managed with ease. There is a tremendous diversity of manufacturers and systems in these categories. These systems can be installed by do-it-yourself home and business owners, or by professionals: integrators, alarm contractors, and others. Ideally, every Device System entering a home, office, retail, medical, or industrial environment will be secured by best practices in the entire lifecycle of the device — including installation and configuration of the device that achieves the "best available security" from the manufactured product.

5 Consumer Tech. Ass'n, *The Connected Home Security System*, https://cta.tech/Membership/Member-Groups/TechHome-Division/Device-Security-Checklist.aspx (last visited Oct. 10, 2018).

6 As major owners and users of networked devices and systems, including an exponentially increasing number of IoT device systems, enterprises of all kinds — government, private sector, academic, and non-profit — have a critical role to play in securing the digital ecosystem. While enterprises often are targets of automated, distributed attacks as well as data exfiltration attempts, their vast systems also can be hijacked to increase the impact of DDoS and other distributed attacks on others. Accordingly, enterprises are among the stakeholders that share responsibility for adequately securing their networks and systems in order to help secure the broader digital ecosystem. The millions of private sector and government enterprises worldwide differ considerably in terms of their technical knowledge and skills, access to resources, and incentives to adopt baseline security practices. Enterprises of all sizes can take their own proactive steps to mitigate ecosystem risk. Such steps can help enterprises protect sensitive data and intellectual property on their networks while also helping to protect the ecosystem at large by reducing the attack surface for botnets. The suppliers and providers that developed this Guide are large global enterprises, and we also provide high-end solutions to secure enterprise networks and mitigate against DDoS attacks and other automated, distributed threats. The "supply" side of this market is robust and growing, and further development of the "demand" side of this market in terms of enterprises of all sizes requesting and negotiating for these services will bring further innovation, sophistication, and cost efficiencies in these services

7 CSDE, ITI, and USTelecom descriptions *infra* p. 41.

8 CTA description *infra* p. 41.

9 For brevity, hereinafter "botnets and other automated, distributed threats" are referred to as "botnets."

10 Andrew Sheehy, *GDP Cannot Explain The Digital Economy*, Forbes (June 6, 2016), https://www.forbes.com/sites/andrewsheehy/2016/06/06/gdp-cannot-explain-the-digital-economy/#47c4db1218db.

11 Irving Wladawsky-Berger, *GDP Doesn't Work in a Digital Economy*, The Wall Street Journal (Nov. 3, 2017) https://blogs.wsj.com/cio/2017/11/03/gdp-doesnt-work-in-a-digital-economy.

12 Paul Tentena, *Artificial Intelligence to Double Digital Economy to 23 Trillion by 2025,* East African Business Week (May 30, 2018), http://www.busiweek.com/artificial-intelligence-to-double-digital-economy-to-23-trillion-by-2025.

13 *See, e.g.,* Catalin Cimpanu, *Sly Malware Author Hides Cryptomining Botnet Behind Ever-shifting Proxy Service*, ZDNet (Sept. 13, 2018), https://www.zdnet.com/article/sly-malware-author-hides-cryptomining-botnet-behind-ever-shifting-proxy-service ("[B]otnets focused on cryptocurrency mining operations have been one of the most active forms of malware infections in 2018."

14 Sam Thielman and Chris Johnston, *Major Cyber Attack Disrupts Internet Service Across Europe and US*, The Guardian, (Oct. 21, 2016), https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service.

15 Michael Newberg, *As Many as 48 Million Twitter Accounts Aren't People, Says Study*, CNBC (Mar. 10, 2017), https://www.cnbc.com/2017/03/10/nearly-48-million-twitter-accounts-could-be-bots-says-study.html.

16 JP Buntinx, *Top 4 Largest Botnets to Date*, Null TX (Jan. 7, 2017), https://nulltx.com/top-4-largest-botnets-to-date.

17 Daniel Newman, *The Top 8 IoT Trends for 2018,* Forbes (Dec. 19, 2017), https://www.forbes.com/sites/danielnewman/2017/12/19/the-top-8-iot-trends-for-2018/#2523096867f7 (citing HIS Markit IoT Trend Watch 2018, *available at* https://ihsmarkit.com/industry/telecommunications.html); *see also* Gartner, *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016* (Feb. 7, 2017), https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016.

18 Jan-Peter Kleinhans, *Internet of Insecure Things: Can Security Assessment Cure Market Failures?*, Stiftung Neue Verantwortung (Dec. 2017), https://www.stiftung-nv.de/sites/default/files/internet_of_insecure_things.pdf.

19 Bill Connor, *Ransomware-As-A-Service: The Next Great Cyber Threat?*, Forbes (Mar. 17, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/03/17/ransomware-as-a-service-the-next-great-cyber-threat/#14a38e5b4123.

20 Andy Greenberg, *The White House Blames Russia for NoPetya, the 'Most Costly Cyber Attack in History'*, Wired (Feb. 15, 2018) https://www.wired.com/story/white-house-russia-notpetya-attribution; Damien Sharkov, *Russia Accused of 1.2 Billion NoPetya Cyberattack*, Newsweek (Feb. 15, 2018) https://www.newsweek.com/russia-accused-massive-12-billion-cyber-attack-807867; CBS News, *What Can We Learn from the Most Devastating Cyber Attack in History?* (Aug. 22, 2018), https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation (dicussing how NotPetya malware caused over $10 billion in damage)

21 Alex Zaharov-Reutt, *Cyber Crime, Data Breaches to Cost Businesses US $8 Trillion Thru 2022*, ITWire (April 25, 2017), https://www.itwire.com/security/77782-$8-trillion-business-cost-from-cybercrime-and-data-breaches-thru-2022.html.

22 Commc'n Sec., Reliability and Interoperability Council IV Working Group 4, *Final Report on Cybersecurity Risk Management and Best Practices* 4 (Mar. 2015), available at https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf (acknowledging "the advantages of a nonregulatory approach over a prescriptive and static compliance regime").

23 *See supra* notes 1–22 and *infra* notes 24–83.

24 Daniel Palmer, *Researchers Discover Huge Crypto Scam Botnet on Twitter*, Coindesk (Aug. 7, 2018), https://www.coindesk.com/researchers-discover-huge-crypto-scam-botnet-on-twitter ("Researchers have uncovered a huge botnet that mimics legitimate accounts on Twitter to spread a cryptocurrency "giveaway" scam.").

25 Tobias Knecht, *A Brief History of Bots and How They've Shaped the Internet Today*, Abusix (Aug. 23, 2017), https://www.abusix.com/blog/a-brief-history-of-bots-and-how-theyve-shaped-the-internet-today.

26 Dustin Volz and Jim Finkle, *U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam*, Reuters (Mar. 2016), https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF.

27 Lee Matthews, *World's Biggest Mirai Botnet Is Being Rented Out for DDoS Attacks*, Forbes (Nov. 29, 2016), https://www.forbes.com/sites/leemathews/2016/11/29/worlds-biggest-mirai-botnet-is-being-rented-out-for-ddos-attacks/#6bdec4cb58ad.

28 *Compare* Elie Bursztein, *Inside the Infamous Mirai IoT Botnet: A Retrospective Analysis*, Cloudflare (Dec. 14, 2017), https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis ("the Mirai assault was by far the largest, topping out at 623 Gbps") with Sean Gallagher, *Federal Grand Jury Indicts 7 Iranians for "Campaign of Cyber Attacks"*, Ars Technica (Mar. 24, 2016) ("At their peak, the DDoS attacks reached 140 gigabits per second").

29 Note that in March 2018, the Mirai botnet's traffic volume record was shattered by attackers targeting GitHub with a DDoS attack reaching 1.35 Terrabytes per second (bps). *See* Lily Hay Newman, *GitHub Survived the Biggest DDoS Attack Ever Recorded*, Wired (Mar. 1, 2018) https://www.wired.com/story/github-ddos-memcached. Notably, the attack did not use a botnet. Instead, the attackers spoofed requests to vulnerable "memcached" servers used to speed up websites, causing victims to be flooded with about 50 times the normal amount of internet traffic. ("Memcached" refers to distributed memory caching systems, which are often used to increase the speed of websites by "caching" data in Random Access Memory rather than relying on external data sources.) Because memcached servers will respond to anyone — including malicious actors — they should not be exposed to the public internet. However, about 100,000 of these servers are exposed and vulnerable; many belong to small businesses and organizations with limited security resources. *See* Liam Tung, *New World Record DDoS Attack Hits 1.7Tbps Days after Landmark GitHub Outage*, ZDNet (Mar. 6, 2018), https://www.zdnet.com/article/new-world-record-ddos-attack-hits-1-7tbps-days-after-landmark-github-outage. Flood attacks of this type that exploit server vulnerabilities have become increasingly popular among bad actors. Only a few days after GitHub survived "the biggest DDoS attack ever recorded" the record was broken again: An Arbor Networks customer was targeted with a similar attack that reached 1.7 Tbps.

30 Cyren, Cyren Cyber Threat Report 8 (Jan. 2017), http://www.vcwsecurity.com/wp-content/uploads/2017/01/Cyren_2017Q1_Botnet_Threat_Report.pdf.

31 Denis Makrushin, *The Cost of Launching a DDoS Attack*, Kaspersky (Mar. 23, 2017), https://securelist.com/the-cost-of-launching-a-ddos-attack/77784.

32 Alfred Ng, *WannaCry Ransomware Loses Its Kill Switch, So Watch Out*, CNET (May 15, 2017), https://www.cnet.com/news/wannacry-ransomware-patched-updated-virus-kill-switch.

33 Ellen Nakashima, *Russian Military was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes*, Washington Post (Jan. 12, 2018), https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?utm_term=.bc4ce7d72018.

34 Andy Greenberg, *Hackers Are Trying to Reignite WannaCry with Nonstop Botnet Attacks*, Wired (May 19, 2017), https://www.wired.com/2017/05/wannacry-ransomware-ddos-attack.

35 CBS News, *What Can We Learn from the Most Devastating Cyber Attack in History?* (Aug. 22, 2018), https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation.

36 U.S. Dep't of Commerce & U.S. Dep't of Homeland Sec., *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* (May 22, 2018), *available at* https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf; Commc'n Sec., 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; ENISA, Botnet Measurement, Detection, Disinfection and Defence (Mar. 7, 2011), https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence; Int'l Telecomm.Union, ITU Botnet Mitigation Toolkit (Jan. 2008), https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit-background.pdf.

37 U.S. Dep't of Commerce & U.S. Dep't of Homeland Sec., *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* 10 (May 22, 2018), *available at* https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.

38 Tim Polk, *Enhancing Resilience of the Internet and Communications Ecosystem*, Nat'l Inst. of Standards and Tech. 7–9 (Sept. 2017) (discussing tools and techniques for DDoS protection, including ingress/egress filtering; on-premise and off-premise DDoS protection), available at https://doi.

org/10.6028/NIST.IR.8192. *See also,* Ctr. for Democracy and Tech, Comments to the NTIA on Promoting Stakeholder Action Against Botnets and Other Automated Threats 2 (Feb. 12, 2018) (agreeing with the NTIA's draft report that "common techniques for botnet mitigation include ingress and egress filtering, re-routing and shaping internet traffic, and isolating devices or other entities."), *available at* https://cdt.org/files/2018/02/CDT-NTIA-Botnet-Comments-Feb-2018.pdf; Commc'n Sec., 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.

[39] *See, .e.g.,* United States, DHS Automated Indicator Sharing (AIS) System, https://www.us-cert.gov/ais (last accessed Oct. 17, 2018); United Kingdom, Cyber Security Information Sharing Partnership (CiSP), https://www.ncsc.gov.uk/cisp (last accessed Oct. 17, 2018); Japan, Cyber Clean Center, https://www.telecom-isac.jp/ccc/en_index.html (last accessed Oct. 17, 2018); New Zealand, CORTEX, https://www.gcsb.govt.nz/our-work/information-assurance/cortex-faqs (last accessed Oct. 17, 2018).

[40] *See* David Strom, *What Is Polymorphic Malware and Why Should I Care?* (Oct. 16, 2015), https://securityintelligence.com/what-is-polymorphic-malware-and-why-should-i-care.

[41] Verizon, 2012 Data Breach Investigations Report 71 (2012), https://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf.

[42] *See* Stephen Sladaritz, *About Heuristics,* SANS Institute 4 (Mar. 23, 2002), *available at* https://www.sans.org/reading-room/whitepapers/malicious/about-heuristics-141 (comparing the two different types of heuristic analysis); *see also* John Aycock, Computer Viruses and Malware 74 (2006) (explaining that the only difference between static and dynamic heuristics is "how the data is gathered" and otherwise the data is identical).

[43] *See, e.g.,* Cisco, Cisco Cognitive Threat Analytics v1 (Feb. 2016), https://dcloud-cms.cisco.com/demo_news/cisco-cognitive-threat-analytics-v1.

[44] Nat'l Inst. of Standards and Tech., *Advanced DDoS Mitigation Techniques (*Oct. 18, 2017) ("For well over a decade industry had developed specifications of techniques and deployment guidance for IP-level filtering techniques to block network traffic with spoofed source addresses"), *available at* https://www.nist.gov/programs-projects/advanced-ddos-mitigation-techniques

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

[46] *Id.*

[47] *See generally*, e.g., Chris Benton, *Egress Filtering FAQ,* SANS Institute (Apr. 19, 2006), *available at* https://www.sans.org/readingroom/whitepapers/firewalls/egress-filtering-faq-1059.

[48] *See* Cisco, *Access Control Lists* (last updated July 17, 2018), https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/asdm79/firewall/asdm-79-firewall-config/access-acls.html.

[49] *See* Cisco, *Policing and Shaping Overview* (last updated Nov. 23, 2017), https://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfpolsh.html.

[50] *See generally*, e.g., Guy Bruneau, *DNS Sinkhole,* SANS Institute (Aug. 7, 2010), https://www.sans.org/reading-room/whitepapers/dns/dns-sinkhole-33523.

[51] *See* Cisco, *Implementing BGP Flowspec* (last updated Jan. 31, 2018), https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r5-2/routing/configuration/guide/b_routing_cg52xasr9k/b_routing_cg52xasr9k_chapter_011.html.

[52] *See* Georgia Tech Researchers, *DNS Changer Remediation Study, Presentation to M3AAWG 27th General Meeting, San Francisco, CA* (Feb. 19, 2013), *available at* https://www.m3aawg.org/sites/default/files/document/GeorgiaTech_DNSChanger_Study-2013-02-19.pdf (last accessed Oct. 17, 2018); *see also* Commc'n Sector Coordinating Council, Botnet Whitepaper 24–25 (July 17, 2017) (listing multiple ways that infrastructure providers can notify users, including email, telephone call, postal mail, text message, web browser notification, walled garden, and other methods such as social media), *available at* https://docs.wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf.

[53] *See* Ctr. for Democracy and Tech, Comments to the NIST Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malwares (Nov. 14, 2011) (expressing concern about the practice of "cutting off or otherwise interfering with a customer's Internet connection" to compel botnet remediation), *available at* https://www.nist.gov/sites/default/files/documents/itl/CDT-Comments-on-BotNet-FRN-11-14-11.pdf; Elec. Frontier Found., Comments to the NIST Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malwares 5 (Nov. 4, 2011) (explaining how uninfected parties could have their internet access affected by quarantine), *available at* https://www.nist.gov/sites/default/files/documents/itl/EFF-Comments-to-BotNet-RFI_11-4-11.pdf.

[54] *See* Commc'n Sector Coordinating Council, Botnet Whitepaper 21 (July 17, 2017), ("No technique is more effective than law enforcement actions that lead to the arrest of the perpetrators. This is the only solution that addresses the root cause of the problem, and not just a symptom… [E]xecuting a botnet takedown requires significant upfront forensic analysis and careful coordination among many stakeholders, often across international borders…. Most botnets are international in nature, requiring resource-intensive and time-consuming cooperation between nations."), *available at* https://docs.wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf.

[55] *See* Robert Wainright and Frank J. Cilluffo, Responding to Cyber Crime at Scale: A Case Study, Europol & the George Washington Univ. Ctr. for Cyber and Homeland Sec. (March 2017), *available at* https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/Responding%20to%20Cybercrime%20at%20Scale%20FINAL.pdf.

[56] *See* SAFECode, Fundamental Practices for Secure Software Development (2018), https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf.

[57] Arora et al., Carnegie Mellon University, An Empirical Analysis of Software Vendors' Patching Behavior: Impact of Vulnerability Disclosure (Jan. 2006) (analyzing incentives of larger vendors relative to other vendors), *available at* https://www.heinz.cmu.edu/~rtelang/disclosure_jan_06.pdf.

[58] *See* SAFECode, Principles for Software Assurance Assessment (2015), *available at* https://safecode.org/publication/SAFECode_Principles_for_Software_Assurance_Assessment.pdf; CA Tech., Veracode, https://www.veracode.com/verified (last accessed June 18, 2018).

[59] Nat'l Inst. of Standards and Tech., NTIA Software Component Transparency, https://www.ntia.doc.gov/SoftwareTransparency (last accessed Nov. 6, 2018).

[60] This section on Devices and Systems draws on Consumer Tech. Ass'n, *Securing Connected Devices for Consumers in the Home — A Manufacturer's Guide* (CTA-CEB33), https://members.cta.tech/ctaPublicationDetails/?id=c12ebabe-84cd-e811-b96f-0003ff52809d (last accessed Oct. 15, 2018).

[61] Early requirements planning and ultimately certification is essential to this process. For example, CTIA manages a certification program for IoT devices, establishing industry requirements for device security on wireless networks and providing a certification program. Details on the program, including requirements and how to certify a device, can be found here: https://www.ctia.org/about-ctia/programs/certification-resources.

[62] *See* Microsoft, What is the Security Development Lifecycle?, https://www.microsoft.com/en-us/sdl/default.aspx (last accessed Oct. 19, 2018).

[63] *See* BSIMM, https://bsimm.com (last accessed Nov. 6, 2018).

[64] For more international standards, *see* Nat'l Inst. of Standards and Tech., *Cryptographic Module Validation Program*, https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards. In addition, NIST has a draft summary of international standards: Nat'l Inst. of Standards and Tech., *Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)*, https://csrc.nist.gov/publications/detail/nistir/8200/draft (last accessed Oct. 10, 2018).

[65] For the current Proposed Recommendation, *see* IETF, Manufacturer Usage Description Specification, https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud (last accessed Oct. 19, 2018).

[66] Cisco, What is Manufacturer Usage Description? (MUD), https://developer.cisco.com/docs/mud/#!what-is-mud (last accessed Oct. 19, 2018).

[67] IEEE, 802.1AR: Secure Device Identity, https://1.ieee802.org/security/802-1ar/ (last accessed Oct. 19, 2018).

[68] Trusted Computing Group, Device Identifier Composition Engine (DICE) Architectures, https://trustedcomputinggroup.org/work-groups/dice-architectures (last accessed Oct. 19, 2018).

[69] For a discussion on updates, *see* Nat'l Inst. of Standards and Tech., *Stakeholder-Drafted Documents on IoT Security,* https://www.ntia.doc.gov/IoTSecurity (last accessed Oct. 10, 2018).

[70] Consumer Tech. Ass'n, *The Connected Home Security System*, https://cta.tech/Membership/Member-Groups/TechHome-Division/Device-Security-Checklist.aspx (last visited Oct. 10, 2018).

[71] U.S. Dep't of Commerce & U.S. Dep't of Homeland Sec., *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* 12–15 (May 22, 2018), *available at* https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.

[72] Cybersecurity Coalition, DDoS Threat Mitigation Profile, https://www.cybersecuritycoalition.org/ddos-framework (last accessed Nov. 14, 2018), *and* Cybersecurity Coalition, Botnet Threat Mitigation Profile, https://www.cybersecuritycoalition.org/botnet-framework (last accessed Nov. 14, 2018).

[73] *See* Commc'n Sec., Reliability and Interoperability Council II Working Group 8, *Final Report on ISP Network Protection* 16 (recommending, *inter alia*, that users should "[c]onfigure [the] computer to download critical updates to both the operating system and installed applications automatically.") (Nov. 2011), *available at* https://www.atis.org/01_legal/docs/CSRICII/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf.

[74] Tim Polk, *Enhancing Resilience of the Internet and Communications Ecosystem,* Nat'l Inst. of Standards and Tech. 13 (Sept. 2017) (citing opinions of participants in the NIST Enhancing Resilience of the Internet and Communications Ecosystem workshop on July 11-12, 2017), *available at* https://doi.org/10.6028/NIST.IR.8192.

[75] Scott Bowen, *Akamai, Defense By Design: How To Dampen DDoS Attacks With A Resilient Network,* Forbes (Sept. 14, 2017) https://www.forbes.com/sites/akamai/2017/09/14/defense-by-design-how-to-dampen-ddos-attacks-with-a-resilient-network/#79144da56f8a.

[76] *See, e.g.*, AT&T, Distributed Denial of Service (DDoS) Defense (2014), *available at* https://www.business.att.com/content/productbrochures/ddos_prodbrief.pdf; Verizon, DDoS Shield Solutions Brief (2016), *available at* http://www.verizonenterprise.com/resources/ddos_shield_solutions_brief_en_xg.pdf; CenturyLink, DDoS Mitigation (2014), *available at* http://www.centurylink.com/asset/business/enterprise/brochure/ddos-mitigation.pdf; Telefonica, Anti-DDoS, https://www.cloud.telefonica.com/en/open-cloud/products/security/anti-ddos (last visited May 14, 2018); NTT, DDoS Protection Service, https://www.ntt.com/en/services/network/gin/transit/ddos.html (last visited May 14, 2018).

[77] *See* discussion *supra* Part 5.A.2(e) (explaining the function of scrubbing centers in mitigating botnets).

[78] Nat'l Inst. of Standards and Tech., *Digital Identity Guidelines* (June 2017), *available at* https://doi.org/10.6028/NIST.SP.800-63-3.

[79] Brian Krebs, *Google: Security Keys Neutralized Employee Phishing*, Krebs on Security (July 23, 2018) https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing.

[80] *See* Microsoft, *Windows XP Support has ended*, https://support.microsoft.com/en-us/help/14223/windows-xp-end-of-support (last visited May 15, 2018).

[81] *See* BSA The Software Alliance, *Seizing Opportunity Through License Compliance: BSA Global Software Survey* 6–7 (2016), http://www.bsa.org/~/media/Files/StudiesDownload/BSA_GSS_US.pdf.

[82] *Id.* at 4 (discussing the "strong correlation" between malware and unlicensed software).

[83] National University of Singapore, *Cybersecurity Risks from Non-Genuine Software, The Link Between Pirated Software Sources and Cybercrime Attacks in Asia Pacific* 6 (Nov. 1, 2017), https://news.microsoft.com/uploads/2017/10/Whitepaper-Cybersecurity-Risks-from-Non-Genuine-Software.pdf ("[I]n many parts of the world, the use of pirated/counterfeit/non-genuine software is a serious contributor to the growth of cyber-risks and is responsible for extensive economic harm and productivity losses. It is also causing a rise in cybercrime attacks and related losses.")

CSDE

Council to Secure the
Digital Economy

securingdigitaleconomy.org