Cyber Crisis: Foundations of Multi-Stakeholder Coordination

CSDE

Council to Secure the Digital Economy

USTELECOM
THE BROADBAND ASSOCIATION

Consumer Technology Association™

In this guide, we lay the foundations for multi-stakeholder coordination during cybersecurity crises that can undermine the security of the digital economy. This guide draws on the diverse international perspectives of CSDE members, as well as their leading practices and real-world actions, to increase incident response readiness, capabilities, and cooperation during catastrophic, crisis-level incidents that call for mobilization of the Information and Communications Technology (ICT) sector.

Cyber Crisis: Foundations of Multi-Stakeholder Coordination

USTELECOM
THE BROADBAND ASSOCIATION

Consumer Technology
Association™

Contents

01 | Executive Summary

THE MEMBERS OF the Council to Secure the Digital Economy (CSDE) cover the complex global internet and communications ecosystem. In this guide, we lay the foundations for multi-stakeholder coordination during cybersecurity crises that can undermine the security of the digital economy. In recent years, we have seen cyber-attacks against power plants, oil and gas companies, financial centers, military organizations, hospitals, governments, and virtually every other institution that supports modern civilization.[1] In the midst of a cybersecurity crisis, government and industry must be prepared to mobilize rapidly and collaborate with relevant responders. This response should be framed in the context of voluntary frameworks where industry leads decisively by leveraging the mature assets and capabilities of Information and Communications Technology (ICT) companies.

Different types of ICT companies, many of which are represented in the CSDE's membership, are likely to be essential during one or more categories of potentially catastrophic cyber events. In order for governments to determine the most relevant, leverageable assets and capabilities of any given company, they should build close working relationships with the companies whose leadership and experience in responding to high-level cyber incidents makes them valuable partners in the global fight against cyber threats. Increasingly, policymakers have recognized the need for international cooperation and coordination to address the growing epidemic of cyber-attacks.

Deploying Security Teams in a Cyber Crisis. As primary drivers of technological innovation and progress across the globe, leading ICT companies have at their collective disposal some of the world's most advanced cybersecurity and incident response assets; these range from state-of-the-art operations facilities with sophisticated mitigation tools, technologies, and processes to experienced teams of cybersecurity experts who are qualified to handle crisis-level events.

The following is not intended to be a comprehensive listing of ICT assets and capabilities, but rather an executive overview of high-value resources and considerations for mitigating cybersecurity incidents.

- **Threat Intelligence Sharing Partnerships** — Omni-directional partnerships across the cybersecurity community facilitate the exchange of vital threat intelligence with both public and private sector partners, and with governmental agencies around the globe.
- **IP Network Operations Center (IP NOC)** — A facility designed to enable management of an IP network to preserve infrastructure integrity and functionality. The IP NOC will typically be staffed by human operators, such as security engineers, who are well-trained at interpreting the data traveling through the network.
- **Security Operations Center (SOC)** — The central team within an organization responsible for cybersecurity. It oversees the human and technological processes and operations necessary to defend against cyber threats.
- **Computer Security Incident Response Team (CSIRT)** — This team is activated only during critical cyber-attacks or vulnerabilities and often employs a structure that is compatible with well recognized best practices that enable a company to swiftly take action during crisis events.
- **Product Security Incident Response Team (PSIRT)** — An entity within an organization that focuses on the identification, assessment, and disposition of the risks associated with security vulnerabilities within the products.[2]

- **Cybersecurity Vulnerability Assessors** — Experts who are trained to discover actual or possible exposure to cyber threats and conduct in-depth analysis of an organization's security posture.
- **Security Engineers and Other Cybersecurity Professionals** — Security engineers are cybersecurity professionals whose job is to protect and mitigate against cyber threats.
- **Subject Matter Experts** — In responding to cyber incidents, companies may leverage input from experts (either in-house or external to the organization) that are recognized for their specialized knowledge in relevant fields of cybersecurity.

Identifying Potential Responders During Cyber Crises. Based on an extensive survey of CSDE members, we developed an understating of the likely roles of different ICT segments in each of the scenarios analyzed. This understanding is represented below and, although subject to changes based on the situational realities "on the ground" during an incident, should serve as effective general guidance for private and public ICT stakeholders.

We recognize that distinct frameworks can provide guidance in different scenarios. Effective incident response requires leveraging the different skill sets of diverse players, and no standard plan or protocol will accommodate every type of crisis. Combating malicious internet traffic, for instance, involves vastly different strategic security considerations, operations, and procedures than mitigating component vulnerabilities. Nonetheless, when CSDE members engage in incident response activities, they aim for common objectives: protecting people, nations, and economies against the worst consequences of significant cyber incidents and decreasing the likelihood of further escalation.

In addition, major companies represented in the CSDE, even if not directly relevant to a resolving a security issue, may be able to help government or industry partners quickly identify relevant ICT companies (infrastructure, software, hardware, security service providers, and others) in the initial triage stage of a potential or actual crisis, in order to facilitate and expedite critical response efforts. Further, these same companies may be in the best position to provide meaningful support in implementing the joint response.

DDoS Attacks

- **Scenarios Examined:** DDoS Botnet Attack; DDoS Server-based Attack
- **Potential Responders:** Situationally relevant Infrastructure Providers; Software Vendors; Hardware Vendors; Managed Security Service Providers

Internet Traffic Hijacking

- **Scenarios Examined:** Border Gateway Protocol (BGP) Hijacking; Domain Name System (DNS) Hijacking
- **Potential Responders for BGP Hijacking:** Situationally relevant Infrastructure Providers; Networking Hardware, Software, and Systems Vendors; Managed Security Service Providers
- **Potential Responders for DNS Hijacking:** DNS Providers; situationally relevant Infrastructure Providers; Networking Hardware, Software, and Systems Vendors

Software Vulnerabilities

- **Scenarios Examined:** Open Source Vulnerabilities; Zero Day Vulnerabilities
- **Potential Responders:** Situationally relevant Software Vendors; Original Software Developers (OSDs); Operating Systems and Firmware Vendors; Virtualization Vendors; Cloud and Hosting Providers; Managed Security Service Providers

Hardware Vulnerabilities

- **Scenarios Examined:** Processor or Component Vulnerabilities
- **Potential Responders:** Situationally relevant Hardware Vendors; Original Equipment Manufacturers (OEMs); Operating Systems and Firmware Vendors; Virtualization Vendors; Cloud and Hosting Providers; Managed Security Service Providers

Software and Hardware Component Backdoors

- **Scenarios Examined:** Injection of Malicious Code in Software and Hardware Components
- **Potential Responders:** Same potential responders as Software and Hardware Vulnerabilities respectively

Malware and Ransomware

- **Scenarios Examined:** Destructive Malware; Ransomware
- **Potential Responders:** Situationally relevant Cloud and Hosting Providers; Software Vendors; Hardware Vendors; Managed Security Service Providers; Incident Response Service Providers

Advanced Persistent Threats (APTs) and Cloud Compromises

- **Scenarios Examined:** Advanced Persistent Threat (APT): Industrial Systems; Cloud Provider Compromise
- **Potential Responders:** Cloud and Hosting Providers; Software Vendors; Hardware Vendors; Managed Security Service Providers; Incident Response Service Providers

Strengthening Relationships and Cooperation. The CSDE considered the global stakeholder community when developing this voluntary guide. In order to harmonize operations in the event of cybersecurity crises that call for private sector mitigations efforts, we will share this guide with a broad set of stakeholders throughout the ecosystem and undertake concerted efforts to encourage participation by key trusted companies in incident response efforts for the security of our digital economy. We will also build awareness of the diverse national and global venues where cyber incident response can be operationalized.

By strengthening the relationships among key stakeholders, as well as developing guides to mitigate specific kinds of cyber threats and vulnerabilities, the CSDE will continue to serve as a critical forum for cyber policy leaders representing global ICT companies that are on the front lines during cyber-attacks and are committed to securing the digital economy.

02 | Introduction

THE MEMBERS OF the Council to Secure the Digital Economy (CSDE) cover the complex global internet and communications ecosystem — including the many human and technical systems that create, deploy, and manage the 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.

In this guide, we lay the foundations for multi-stakeholder coordination during cybersecurity crises that can undermine the security of the digital economy. This guide draws on the diverse international perspectives of CSDE members, as well as their leading practices and real-world actions, to increase incident response readiness, capabilities, and cooperation during catastrophic, crisis-level incidents that call for mobilization of the Information and Communications Technology (ICT) sector.

We recognize that distinct frameworks can provide guidance in different scenarios. Effective incident response requires leveraging the different skill sets of diverse players, and no standard plan or protocol will accommodate every type of crisis. Combating malicious internet traffic, for instance, involves vastly different strategic security considerations, operations, and procedures than mitigating component vulnerabilities. Nonetheless, when CSDE members engage in incident response activities, they aim for common objectives: protecting people, nations, and economies against the worst consequences of significant cyber incidents and decreasing the likelihood of further escalation.

Global Cyber Crises: More Frequent, More Costly, and More Dangerous. The digital economy is producing immense benefits for the world that must be defended against aggressive actions and potentially devastating cyber events. By some estimates, the digital economy may already represent 20% of global economic value,[3] and although GDP alone cannot capture the full worth of the digital economy, the projected value of the digital economy by 2025 is $23 trillion — almost a quarter of global GDP.[4] The digital economy has generated quality-of-life improvements on every continent, created whole new industries and millions of jobs, and increased efficiency in every sector.

At the same time, the asymmetry between the relatively low cost of launching highly disruptive cyber-attacks and the high cost to defend against such attacks, among other factors, has created harmful incentives for sophisticated actors, including nation states that wish to project power and influence in global affairs. In recent years, we have seen criminal and politically motivated attacks on critical infrastructure, as well as other illicit operations such as cyber espionage and ransoming of critical data. These emerging trends could result in massive economic damage and undermine confidence in the digital economy, which is an outcome the CSDE was created to prevent.

The economic and public safety consequences of cyber-attacks have increased severely in recent years. An attack against a cloud service provider could cause tens of billions of dollars in damage, and one study estimates that a single cloud event can cost up to $120 billion, a figure that exceeds some of the worst natural disasters.[5] We have seen cyber-attacks against power plants, oil and gas companies, financial centers, military organizations, hospitals, governments, and virtually every other institution that supports modern civilization.[6]

It is clear that cyber-attacks have reached the level of a sustained crisis in some parts of the world. For example, in 2015, a cyber-attack caused people in Ukraine to lose electricity for six hours in the middle of winter.[7] In 2017, an attack against the same country's financial systems escalated into an international epidemic that caused over $10 billion damage worldwide.[8] This was the costliest cyber-attack in history,[9] but much more damaging attacks are possible.

Researchers continue to discover malware targeted against specific geopolitical targets in many parts of the world.[10] In a shared internet and communications ecosystem, attacks targeted at specific nations can and often do have spillover effects that are damaging for broad sets of stakeholders — not just the intended targets.[11] Hence, whether dealing with hacking groups sponsored by nation states with geopolitical ambitions or sophisticated cybercriminal organizations with profit-driven goals, like-minded governments and industry alliances have enormous incentives to curtail the most damaging actions in cyberspace and unite against common threats to the shared digital ecosystem.

It is not merely a matter of ethical necessity and building mutually beneficial relationships; it is also a matter of protecting each nation's economic and security interests.

Industry Provides Leadership in a Cyber Crisis. The CSDE recognizes the need for industry leadership and collaboration with government partners during major cyber incidents. As the capabilities of well-financed and sophisticated malicious actors reach new levels of maturity, dangers in the cyber threat environment increasingly pose global and ecosystem-wide economic security challenges that exceed the individual response capabilities of any single company or industrial sector.

The widespread and consequential nature of the most serious cyber threats requires ICT companies — particularly companies with assets and capabilities that may be necessary to support incident response during cyber incidents — to recognize shared dependencies and responsibilities as stewards of the digital economy and jointly coordinate actions necessary for immediate response to and recovery from catastrophic scenarios. The CSDE's diverse and global members, which include ICT companies across the internet and communications ecosystem, are excellently positioned to provide the guidance, insight, and leadership needed for their respective ecosystem segments.

In the midst of a cybersecurity crisis, government and industry must be prepared to mobilize rapidly and collaborate with relevant responders. This response should be framed in the context of voluntary frameworks where industry leads decisively by leveraging the mature assets and capabilities of ICT companies.

Project Phases and Methodology. The CSDE's work on industry responses to a cyber crisis builds on findings and recommendations in the November 19, 2014 National Security Telecommunications Advisory Committee (NSTAC) Report to the President on Information and Communications Technology Mobilization[12] and the June 2016 Homeland Security Advisory Council Final Report of the Cybersecurity Subcommittee on Incident Response,[13] as well as similar calls to action in other jurisdictions, such as European Union Agency for Network and Information Security (ENISA) publications on cyber crisis cooperation.[14]

This report documents the CSDE's efforts to identify key resources among global ICT companies across two distinct phases.

- During the first phase, the CSDE identified categories of cyber threats and vulnerabilities that may require the mobilization of the ICT sector. These categories were chosen in consultation with experts and sources from industry, government, and civil society.
- In the second phase, the CSDE conducted a survey of member companies, leveraging the expertise of leading cybersecurity professionals and other institutional resources, to identify (1) incident response assets and capabilities that ICT stakeholders may provide to mitigate a crisis scenario and (2) potential industry responders in select crisis scenarios. *See* Appendix A for the survey scenarios.

Producing this guide reflects our broader commitment to reducing barriers to cooperation in cyber crises. We will share this guide with a broad set of stakeholders throughout the ecosystem and undertake concerted efforts to encourage participation by key trusted companies in incident response efforts for the security of our digital economy.

03 | Overview of Global ICT Segments Represented in the CSDE

IN THIS SECTION, we describe the different types of ICT companies that are represented in the CSDE's membership and are likely to be essential during one or more categories of potentially catastrophic cyber events. We recognize that all ICT companies, including those not described in this section, have a role to play in securing the global digital ecosystem against a range of cyber threats and vulnerabilities.

To the extent that the types of providers described in this section may not have all of the assets and capabilities needed to respond to a crisis, they will sometimes have formal or informal working relationships with other parties that can help mitigate the crisis.

Infrastructure Providers. The internet is a complex "system of systems" with many different layers of infrastructure that enable connectivity and operability. Represented among the CSDE's diverse membership are leading global ICT companies that provide the infrastructure that enables internet access and content delivery and, along with other stakeholders in the digital economy, their capabilities would likely be critical in mitigating specific types of cyber crisis scenarios.

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 a large variety of security solutions, including managed services, whereby the provider takes an active role in mitigating threats to their customers.

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, while also providing an additional layer of security.

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 distributed cyber-attacks and provides additional mitigation capabilities. In essence, cloud services provide access to a wide range of content and functions, as well as an incremental layer of security, outside of the infrastructure provided by an ISP.

Software Developers and Vendors. Software is an increasingly ubiquitous element of the digital ecosystem. Accordingly, many types of software developers and vendors are represented in the CSDE. In the event of a cyber crisis, software developers and vendors may play multiple roles depending on the types of products and services they offer customers and the nature of the crisis, among other situation-specific considerations.

In general, software may be divided into systems and applications. Systems enable users to operate and manage hardware. Applications are programs that enable an incredibly wide range of computing functions. Every single day, millions of people download applications onto their personal smart phones and endpoint devices. Application software includes antivirus programs and other programs designed to improve security.

Components of software may be proprietary or open source. Proprietary software components have legal conditions on their use and their source code may be a closely guarded company secret, in order to protect the rights and

commercial interests of the owners. Open source software components, as the name implies, have a source code that is accessible to the general public, and it can be used or modified by any interested party with sufficient technical skills.

In some scenarios, developers of propriety software may have specific insights relevant to mitigating a security issue. Even if the issue stems from vulnerabilities in software components that no ICT company owns, a large software company's institutional knowledge and experience mitigating software-based risks may be beneficial to incident response and recovery efforts.

Hardware Manufacturers and Vendors. For purposes of this report, hardware refers to the tangible components of ICT systems, including devices as well as network equipment that connects systems across end users' homes or across the globe. The complexity and security considerations associated with hardware will vary greatly based on its intended use and relationship to software and network components of the ecosystem.

The CSDE's diverse membership includes original equipment manufacturers (OEMs) and hardware vendors. During a crisis that originates with a hardware-based vulnerability, the CSDE members that create hardware components may have important insights and mitigation capabilities.

Some manufacturers create hardware specifically for systems of devices. 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.

Other manufacturers create hardware for infrastructure or advanced industrial processes that increase efficiencies across numerous sectors of the global economy. Based on the criticality of the hardware in specific systems or process to ecosystem-wide priorities, different companies are likely to have varying levels of appropriate risk management capabilities.

Security Service Providers. Professional security services offer customers key advantages in the event of a crisis. The CSDE's membership includes Managed Security Service Providers (MSSPs) and Incident Response Service Providers.

Managed Security Service Providers (MSSPs) offer remote IT management and monitoring services for their customers, either complementing in-house security teams or providing broad sets of security solutions. MSSPs serve many different markets including large companies, governments, nonprofits, and small and medium-sized business, among others. Services offered by MSSPs may include services such as intrusion detection and filtering solutions (e.g., firewalls), as well as unified threat management. A number of CSDE members offer fully managed end-to-end solutions to increase network security. MSSPs may offer some services that help mitigate cyber-attacks known to compromise large organizations, for example data breaches and ransomware, as well recover from those types of incidents.

Incident Response Service Providers help customers respond to an incident with the goal of reducing damage and exposure. They use threat intelligence to help customers make decisions during a crisis and develop custom strategies to identify the attacker and get to the root cause of an incident. Incident Response Service Providers are typically hired on a retainer. Because time and geographic presence are of the essence during a crisis, providers may have the capability to assist customers remotely while traveling to their physical locations.

04 | Private Sector Cyber Crisis Assets and Capabilities

COMMERCIAL OFFERINGS in the global ICT ecosystem are highly complex and dynamic. Companies across the world will evolve their business models, services, and products — and therefore their role within the ecosystem — based on market incentives, competition, technological evolution and convergence, and opportunities for innovation, among other considerations that lead to new strategies for delivering value to different sets of customers.

In recent years, technological advances such as cloud migration have led to increased convergence between the technological capabilities of different types of service providers, manufacturers, developers, and vendors whose offerings depend on shared resources and functionality. Previously unrelated technologies are now closely linked via underlying digital platforms enabled by diverse connective infrastructure. It is a well-observed tendency that, over time, technologies tend to become increasingly interoperable to expand their functions, security, and efficiency, akin to how biological systems evolve and adapt in response to their environments.

This section offers a snapshot of the assets and capabilities that leading ICT companies may have during a crisis, if a catastrophic incident were to occur today. In the event of a crisis, the assets and capabilities of different companies could overlap to varying extents. For example, leading ISPs offer customers some of the same services as security vendors. Companies that sell and manufacture hardware for systems and devices may also develop software components. Providers of Industrial Control Systems (ICS), for instance, incorporate software, firmware, hardware, and network components.

In order for governments to determine the most relevant, leverageable assets and capabilities of any given company, they should build close working relationships with the companies whose leadership and experience in responding tow high-level cyber incidents makes them valuable partners in the global fight against cyber threats.

All types of ICT companies must be vigilant of unique security concerns affecting their constituencies across relevant segments of the digital ecosystem. The assets and capabilities of ICT companies during catastrophic cyber events generally include the following security teams and professionals:

- **Threat Intelligence Sharing Partnerships**
- **IP Network Operations Center (IP NOC)**
- **Security Operations Center (SOC)**
- **Computer Security Incident Response Team (CSIRT)**
- **Product Security Incident Response Team (PSIRT)**
- **Cybersecurity Vulnerability Assessors**
- **Security Engineers and Other Cybersecurity Professionals**
- **Subject Matter Experts**

Roles of Security Teams in a Cyber Crisis. As primary drivers of technological innovation and progress across the globe, leading ICT companies collectively have at their disposal some of the world's most advanced cybersecurity and incident response assets; these range from state-of-the-art operations facilities with sophisticated mitigation tools, technologies, and processes to experienced teams of cybersecurity experts who are qualified to handle crisis-level events.

Given the vast array of global companies and institutional cultures in the digital ecosystem, these assets and their associated capabilities can be implemented differently by individual organizations and may be referred to by diverse names within each organization. Nonetheless, they share key functions and operational structures in common that make them recognizable across a variety of nomenclatures.

The following is not intended to be a comprehensive listing of ICT assets and capabilities, but rather an executive overview of high-value resources for mitigating cybersecurity incidents that, absent rapid and effective mitigation, could have devastating consequences for public safety, security of nations across the world, and the global digital economy.

Threat Intelligence Sharing Partnerships

Threat intelligence sharing partnerships across the cybersecurity community facilitate the exchange of vital threat intelligence with both public and private sector partners, and with governmental agencies around the globe. Partners may share critical non-public indicators — such as malicious IP addresses and domain names, malware used in attacks, and unique tactics used by advanced threat actors — to better protect clients, partners and the public. While no single organization, public or private, has complete visibility into the threat landscape, the breadth of visibility by the largest ICT companies is compelling. Further these same companies arguably have the most extensive range of information-sharing relationships. The individual and collective visibility of these companies provides the means to fill in gaps in both regional and global visibility and collaborate in real-time — thereby enabling threat responders to more quickly and effectively remediate threats.

IP Network Operations Center (IP NOC)

An IP NOC is a facility designed to enable management of an IP network to preserve infrastructure integrity and functionality, minimize service disruptions and downtime which may be caused by cyber incidents, and meet the requirements of service-level- agreements. The IP NOC provides situational awareness of the network's traffic and performance on an ongoing basis through monitoring and analysis.

The facility may have large screens that display visual representations of the network's status and operations. The IP NOC will typically be staffed by human operators, such as security engineers, who are well-trained at interpreting the data traveling through the network and may receive notifications from customers or other parties about disruptions or anomalous activity. The IP NOC may also be able to contact customers in case of an emergency.

Global infrastructure providers' IP NOCs have at their disposal systems and applications necessary to perform traffic management; assist customers or peers with troubleshooting; distribute software updates; and manage infrastructure such as servers, routers, and domain names.[15]

Security Operations Center (SOC)

An SOC is the central team within an organization responsible for cybersecurity. It oversees the human and technological processes and operations necessary to defend against cyber threats. An SOC's functions may include all categories of activities identified in the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover.[16]

SOCs of large companies may be comprised of multiple teams, each equipped with a specialty that complements the others. These groups can work in tandem to respond to large-scale cyber incidents. A Command SOC team may be designated to coordinate the actions of other teams. Some teams may function autonomously for strategic purposes.

In the case of large companies, the SOC will typically have at least one physical headquarters or facility with specialized equipment that allows the team to carry out its mission. For example, an SOC can monitor and analyze network activity, including in the cloud, as well as endpoints, applications, and connected systems, in order to provide a source of intelligence to identify security incidents.

In addition to helping identify security incidents, some SOCs have advanced capabilities such as digital forensics and reverse-engineering, which allow them to analyze a threat in-depth and provide valuable intelligence to combat cyber threats.

In a cyber crisis, the primary focus of a Command SOC team is to quickly activate the relevant Computer Security Incident Response Team (CSIRT) (see below) to respond to the incident's specifics and, when appropriate, stand-down the response team as quickly as possible to return to business as usual. The Command SOC is also the entity that generally determines when to contact parties outside the company. Typically, the response team will only be activated during a significant cyber-attack or large-scale cyber incident.

Computer Security Incident Response Team (CSIRT)

This team is activated only during critical cyber-attacks or vulnerabilities and often employs a structure that is compatible with recognized best practices that enable a company to swiftly take action during crisis events. The role of the CSIRT is to limit damage, facilitate recovery efforts, and take steps to mitigate against future incidents. The human element of a CSIRT are security experts who can coordinate incident response across an array of different cyber incidents determined by the needs of the organization and its constituencies.

CSIRT staff may be trained to handle situations that could lead to potentially catastrophic incidents for public safety and national security. The CSIRT will have specialized knowledge of the threats facing the company and its customers, as well as response strategies tailored to the company' s resources and priorities during a cyber crisis.

CSIRT strategies for responding to cyber crises evolve along with technology and may be updated regularly, shared with team members, and tested often throughout the year in table top and simulation exercises. Strategic considerations for large companies include the people, processes, and tooling required for the team to respond to heightened levels of cybersecurity incidents.

Product Security Incident Response Team (PSIRT)

A Product Security Incident Response Team (PSIRT) is an entity within an organization that focuses on the identification, assessment, and disposition of the risks associated with security vulnerabilities within the products, including offerings, solutions, components, and/or services which an organization produces and/or sells.[17] Software and hardware vendors' PSIRTs are the teams that coordinate the disclosure of those vulnerabilities to their customers.

Cybersecurity Vulnerability Assessors

A cybersecurity vulnerability assessment (CVA) is an in-depth analysis of an organization's security posture conducted by experts who are trained to discover actual or possible exposure to cyber threats. By conducting CVAs, an organization can make informed decisions about how to mitigate risk and manage resources cost-effectively in order to prioritize the most serious types of threats. CVAs may assess the attack surfaces of networks, devices, systems and application software, and other ICT assets. These capabilities help security leaders identify and remediate security flaws, covering their entire digital and physical ecosystem.

Companies may have the capability to conduct CVAs in-house or they may contract with third parties to obtain these services. Penetration testing, a feature of some assessments, is generally carried out by autonomous teams

of experienced hackers hired to break into organizations and uncover risky vulnerabilities that threat actors may take advantage of. Similarly, Red Team assessments involve hiring hackers to break into an organization, but often more closely mirroring a real-world situation, where the goal is to get in by any means necessary, rather than to uncover the greatest number of vulnerabilities. In general, the hired hackers can do what criminal hackers can do, but with the goal of helping security leaders harden their defenses and protect their most important assets.

Security Engineers and Other Cybersecurity Professionals

Security engineers are cybersecurity professionals whose job is to protect and mitigate against cyber threats. This an advanced-level job according to the CyberSeek model developed by the National Initiative for Cybersecurity Education (NICE), a partnership led by NIST between government, industry, and academia to promote cybersecurity workforce development.[18] Security engineers are often on the front lines during a cyber-attack against global ICT companies. For example, network security engineers have essential skills for resolving issues such as DDoS attacks and BGP hijacking.

Many cybersecurity professionals in the employ of ICT companies have skills and knowledge that may be leveraged during cybersecurity events. The CyberSeek model provides a comprehensive overview of the different types of cybersecurity professionals.[19] The individuals employed or contracted to these companies will clearly align with that company's products, services or needs.

Subject Matter Experts (SMEs)

In responding to cyber incidents, companies may leverage input from experts (either in-house or external to the organization) that are recognized for their specialized knowledge in relevant fields of cybersecurity. For example, an ISP may leverage the knowledge of an in-house DNS expert to ensure proper configuration of domain names. When dealing with newly discovered hardware or software vulnerabilities, a vendor may consult leading security researchers. As technology grows more complex, we will likely continue to see greater degrees of specialization among experts.

Technical experts aside, other types of SMEs will likely provide input before finalizing courses of action. Considerations such as privacy, legal and regulatory considerations, business operations, communications with customers, collaboration with governments across the globe, and other subjects may be relevant to incident response.

05 | Public-Private Coordination in Cyber Crisis Scenarios

AS A MAJOR VOICE of global ICT companies, the CSDE can play a leading role in promoting collaboration among industry and government to prepare for cyber crises. In addition, we can work with governments and industrial bodies to harmonize international frameworks.

Events Prior to Joint Cyber Crisis Response. As a matter of course, information-sharing is ongoing among and between these companies. The laws and policies governing information-sharing procedures for cyber threats can vary from country to country. Nonetheless, global efforts are currently underway among like-minded governments to increase information-sharing.[20]

Enterprises must collaborate within their own sectors and with government to share knowledge of pertinent cyber threats. Indeed, enterprises are often the first to discover a cyber threat because their systems are directly impacted when an incident occurs. Due to their unique positions in the cyber ecosystem, they have a capability to alert industry and government when a serious incident occurs and share critical information needed to recognize emerging threat patterns in the ecosystem.[21] Generally, large enterprises have more access to the institutional knowledge, technical training, and other resources needed to collaborate effectively with industry and government. However, smaller enterprises in the aggregate can also contribute to evidence of emerging cyber threat patterns.[22]

In many countries, enterprises can share information with an Information Sharing Analysis Center (ISAC) or functional equivalent.[23] The ISAC or its equivalent can then share the information with trust groups to the extent permitted by each country's laws. At this stage, a determination must be made whether the incident is serious enough to merit the involvement of leading ICT companies.

Considerations in Supporting Joint Cyber Response. Ultimately, each company must decide when and how to deploy assets and capabilities it considers appropriate to mitigate a cybersecurity incident, and the extent to which the company will either request assistance or provide assistance to others. This decision is made using a multi-factored analysis, which can include policy and legal considerations, as well as practical realities on the front lines of cyber-defense. Once acting in collaboration with other ICT partners, some companies voluntarily adopt industry protocols that help guide multi-party operationalization in a crisis. For example, a number of CSDE members are charter members of ICASI, which developed the *Unified Security Incident Response Plan* (USIRP).

Companies' decisions may be informed by diverse opinions from experts in multiple countries, and while there is no single definition of a cyber crisis that will apply in every scenario, a number of helpful considerations have been identified by experts.

For example, the NSTAC report calls for leading ICT companies to be mobilized in "widespread" or "particularly grave" events.[24] A widespread event can mean "complete infiltration of a sector or substantial foothold across two or more sectors."[25] A grave event can mean "a critical dependency is completely overwhelmed and request for resources exceeds available capabilities."[26]

Similar concepts are found in the incident response strategies of other jurisdictions. ENISA's *Strategies for Incident Response and Cyber Crisis Cooperation* defines a crisis as "an extraordinary event that differs from the normal and involves serious disturbance or risk for disturbance of vital societal functions"; "an abnormal and unstable situation that threatens an organisation's strategic objectives, reputation or viability"; and an "event that strikes at the heart of the organization".[27]

Appendix A contains twelve (12) scenarios identified by the CSDE that could escalate to a scale that causes a number of ICT companies to take coordinated action against a common threat. These scenarios are based on the following types of cyber incidents:

- **DDoS Botnet Attack**
- **DDoS Server-based Attack**
- **Border Gateway Protocol (BGP) Hijacking**
- **Domain Name System (DNS) Hijacking**
- **Software Vulnerabilities: Open Source**
- **Software Vulnerabilities: Zero Day**
- **Hardware Vulnerabilities: Processor Architectures**
- **Injection of Malicious Code in Software and Hardware Components**
- **Destructive Malware**
- **Ransomware**
- **Advanced Persistent Threat (APT): Industrial Systems**
- **Cloud Provider Compromise**

Roles of ICT Companies During Cyber Crises. When a cyber threat or vulnerability presents itself, the relevant ICT companies can self-select into groups capable of rapidly mobilizing critical private sector assets to effectively respond in the event of a major cyber emergency. To the extent practical, industry response strategies may be pre-coordinated while recognizing the evolving and dynamic nature of the threat.

Based on an extensive survey of CSDE members, we developed an understating of the likely roles of different ICT segments in each of the scenarios analyzed. This understanding is represented below and, although subject to changes based on the situational realities "on the ground" during an incident, should serve as effective general guidance for private and public ICT stakeholders.

In addition, major companies represented in the CSDE, even if not directly relevant to a resolving a security issue, may be able to help government or industry partners quickly identify relevant ICT companies (infrastructure, software, hardware, security service providers, and others) in the initial triage stage of a potential or actual crisis, in order to facilitate and expedite critical response efforts. Further, these same companies may be in the best position to provide meaningful support in implementing the joint response.

DDoS Attacks

- **Scenarios Examined:** DDoS Botnet Attack; DDoS Server-based Attack
- **Potential Responders:** Situationally relevant Infrastructure Providers; Software Vendors; Hardware Vendors; Managed Security Service Providers

Internet Traffic Hijacking

- **Scenarios Examined:** Border Gateway Protocol (BGP) Hijacking; Domain Name System (DNS) Hijacking
- **Potential Responders for BGP Hijacking:** Situationally relevant Infrastructure Providers; Networking Hardware, Software, and Systems Vendors; Managed Security Service Providers
- **Potential Responders for DNS Hijacking:** DNS Providers; situationally relevant Infrastructure Providers; Networking Hardware, Software, and Systems Vendors

Software Vulnerabilities

- **Scenarios Examined:** Open Source Vulnerabilities; Zero Day Vulnerabilities
- **Potential Responders:** Situationally relevant Software Vendors; Original Software Developers (OSDs); Operating Systems and Firmware Vendors; Virtualization Vendors; Cloud and Hosting Providers; Managed Security Service Providers

Hardware Vulnerabilities

- **Scenarios Examined:** Processor or Component Vulnerabilities
- **Potential Responders:** Situationally relevant Hardware Vendors; Original Equipment Manufacturers (OEMs); Operating Systems and Firmware Vendors; Virtualization Vendors; Cloud and Hosting Providers; Managed Security Service Providers

Software and Hardware Component Backdoors

- **Scenarios Examined:** Injection of Malicious Code in Software and Hardware Components
- **Potential Responders:** Same potential responders as Software and Hardware Vulnerabilities respectively

Malware and Ransomware

- **Scenarios Examined:** Destructive Malware; Ransomware
- **Potential Responders:** Situationally relevant Cloud and Hosting Providers; Software Vendors; Hardware Vendors; Managed Security Service Providers; Incident Response Service Providers

Advanced Persistent Threats (APTs) and Cloud Compromises

- **Scenarios Examined:** Advanced Persistent Threat (APT): Industrial Systems; Cloud Provider Compromise
- **Potential Responders:** Cloud and Hosting Providers; Software Vendors; Hardware Vendors; Managed Security Service Providers; Incident Response Service Providers

Advance Planning for Joint Cyber Response:

The scenarios highlighted above occur on a regular basis, albeit at a smaller scale not requiring the level of mobilization contemplated within this report. These smaller-scale events provided the insights into the likely class of responders that might be required under more extreme circumstances. What these scenarios cannot tease out with any precise definition is the specific names of the companies within these categories that might be situationally relevant for any given event. Below, we look at two examples and expand on the escalation process that might lead to a Joint Cyber Response.

Example: Mitigating Software and Hardware Vulnerabilities

Recent developments such as the exponential growth of connectivity have shown the world that a vulnerability in either software or hardware components can have significant consequences that reverberate throughout the digital ecosystem. A single security flaw in a piece of code or hardware component can potentially impact a wide range of products. While coordination efforts are notionally the same for software and hardware ICT components, mitigating hardware vulnerabilities can require considerable multi-party coordination and may present operational challenges that are unique to the hardware context. The multi-party coordination effort for a vulnerability in a technology owned and manufactured by the vendor leading the process might entail different processes than one in which a broader collaboration is needed and there is no one distinct owner/manufacturer of the technology (e.g., protocol-level vulnerabilities).

Responding to incidents involving vulnerable ICT components or software, whether in device systems or infrastructure, may require an understanding of factors such as how hardware and software components and systems are integrated and the environment in which components are deployed. For example, software companies including operating systems and firmware vendors and virtualization vendors may be integral to the process of developing and testing a mitigation for a hardware-based vulnerability (in a process often termed “Multi-Party CVD”, led by the hardware manufacturer). Cloud providers also play an important role in mitigation development and testing for infrastructure they operate.

Four of the scenarios outlined above fall predominantly in the Software/Hardware domains: Software Vulnerabilities-Open Source, Software Vulnerabilities-Zero Day, Hardware Vulnerabilities-Processor Architectures, and Injection of Malicious Code in Software and Hardware Components.

In the case of a Hardware Vulnerability, usually the Hardware Company manufacturing the component, technically knowledgeable of the product, is best situated to lead the coordination effort. Relevant ecosystem partners collaborating with the hardware manufacturer in the Multi-Party coordination effort will also likely be situationally relevant and take part in the mitigation development and testing effort, as needed. Such parties may include other manufacturers of directly-affected hardware products (if applicable), vendors involved in assembling the product into different systems and products (OEMs) or partners integrating the components in certain technical environments that require further consideration (e.g., operating system, cloud environments, software and firmware development). Please note: the vast majority of cyber incidents in this context are addressed, and mitigations are developed, as part of a Multi-Party CVD process led by the hardware manufacturer in collaboration with the Vendor/Partner ecosystem.

In other, different, Multi-Party CVD settings (software or hardware) in which there is no clear owner of the technology/manufacturer best-situated to lead the coordination efforts (for example, in certain protocol-level vulnerabilities),

and depending on the nature of the attack, a broader collaboration within the ecosystem may be needed to develop, test, and release mitigations. In this stage, ICT companies may consider reaching out to like-companies to explore if they (or their partner ecosystems) have insights into mitigation or containment strategies in a Multi-Party CVD effort encompassing a broader set of representatives from the technological ecosystem. Such outreach might extend to entities like ISACs/ISAOs or other comparable venues.

The need to mobilize peer (and potentially competitor) hardware/software companies to address and mitigate events is already understood, and protocols to do so have been proposed and are already in place.

For example, a number of CSDE members are charter members of ICASI, which developed the *Unified Security Incident Response Plan* (USIRP). The Unified Security Incident Response Plan (USIRP) is one of the primary means by which ICASI fulfills its mission of enhancing the global security landscape. Comprising a trusted forum and supporting processes, procedures, and tools, the USIRP enables Security Incident Response Teams (SIRTs) from ICASI member companies as well as select, invited outside organizations to collaborate quickly and effectively to resolve complex, multi-stakeholder Internet security issues (such as in protocols)[28] in which there is no clear one owner/manufacturer leading the coordination effort and broader collaboration is needed.

Some of the types of issues addressed in this environment are reflected below:

COORDINATED VULNERABILITY DISCLOSURE (CVD)

CSDE's member companies, together with security researchers in many countries across the world, are working constantly to discover and address vulnerabilities in technology (software, firmware, hardware) and develop protective measures to mitigate against the risks posed by those and other vulnerabilities. The globally intertwined nature of technology and international collaboration that CVD and Multi-Party CVD entails supports the development, adoption and harmonization of consensus-driven international best practices and standards that align and are informed by industry best practices.[29]

The complexity of ICT components and software that are essential to the digital economy, as well as the security of nations and global infrastructure, creates incentives for trusted researchers in the cybersecurity community to collaborate across sectors and often with government partners. At the same time, companies from all sectors have a responsibility to carefully limit the spread of information concerning the vulnerability that could be misused by malicious actors to create harm while mitigations are not available.

ICT components and software may have security vulnerabilities that expose systems to risk, which may result in economic and national security challenges. To address these challenges, as well as more mundane security vulnerabilities, the process known as CVD has emerged to minimize harm to the global community. In the past, CVD was focused on software and software-based products. But the rapid transformation of the digital ecosystem, among other security-related developments, has led to increased development on hardware vulnerability and Multi-Party CVD disclosure best practices.

The security rationale for CVD is commonsensical: disclosing vulnerabilities before mitigations are ready and available for end users makes exploitation more probable. To reduce the likelihood of widespread exploitation, CVD limits disclosure of vulnerabilities at each step to those stakeholders that are essential contributors to mitigation. At the same time, the CVD process seeks to promote reasonably fast-paced development of mitigations and strategies to distribute those mitigations effectively.

The CVD process guides vendors, security researchers, and other stakeholders in the digital economy to cooperate on the development of mitigations addressing a given vulnerability while simultaneously limiting disclosure of information concerning that vulnerability until such time as mitigations and information can be made available to the public in a coordinated manner.[30] The CVD process is consistent with NIST's Cybersecurity Framework, which recommends the establishment of processes to "receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers)."[31] The National Telecommunications and Information Administration (NTIA) has collaborated with industry and global stakeholders represented in the Forum of Incident Response and Security Teams (FIRST) to develop guidelines and practices for multi-party vulnerability coordination and disclosure.[32] There are also widely-adopted international standards focusing on Coordinated Vulnerability Handling and Disclosure, ISO/IEC 30111 (2013) (in renewal stages, 2019) and ISO/IEC 29147 (2018).

During incident response, time is often of the essence. Sometimes, patching hardware vulnerabilities can be very complex, requiring collaboration and complex coordination between multiple vendors (a process often referred to as "Multi-Party CVD") to develop and test mitigations and deliver them to end users.[33] In some cases, various approaches to mitigation based on respective architectures are considered. This was the case, for example, of the Spectre and Meltdown exploits which took advantage of a common feature in modern processors (while being relatively difficult to exploit). In some cases, it may be appropriate to deploy temporary workarounds until more enduring fixes and mitigations are available. Over time, even very complicated challenges can often be solved but may require a longer period of time for coordination in complex environments.[34]

If a significant cyber-attack occurs before appropriate mitigations are ready, stakeholders may disclose information and guidance necessary to minimize harm to the public, while withholding information that bad actors could use to make the situation worse. This is a careful balancing act and requires careful coordination among the relevant parties. Intermediaries such as national CERTs can sometimes help stakeholders in the CVD process cooperate effectively on shared security goals.

SOFTWARE AND HARDWARE MITIGATIONS DISTRIBUTION

In the case of software vulnerabilities, mitigations distribution may require nothing more from a technical perspective than updating the relevant code libraries. Often, the bigger challenge is persuading users or other properly authorized decision-makers to accept updates in a timely and coordinated manner. Mitigating hardware vulnerabilities, however, may require coordination among manufacturers, suppliers, technicians, and vendors that fill distinct roles necessary to secure the hardware components of a system.

One the one hand, there are easy updates on smart phones and computers that users are familiar with, as well as hassle-free software as a service (SAAS) updates in the cloud environment. On the other hand, many IoT devices would need physical upgrades that are commercially unfeasible and, in some cases, may cost more to deploy than the device is worth. This is why it is important to design devices securely in the first place. The CSDE's *International Anti-Botnet Guide* provides relevant guidance on secure-by-design development and mitigations strategies for device systems. In addition, the CSDE C2 Consensus on IoT Device Baseline Security is the broadest and most technically deep industry consensus on IoT security worldwide. You can download these documents on our official website: securingdigitaleconomy.org.

An important factor in a hardware component manufacturer's capability to distribute mitigations is how the component is integrated into device systems or infrastructure. A component vendor that has no direct relationship with the customers who own device systems or infrastructure will probably collaborate with additional stakeholders (like OS vendors and OEMs) to distribute mitigations to end users. A vendor that produces all components for a device — for example, a simple IoT device or industrial control system (ICS) — may in some circumstances have the ability to handle the distribution on its own.

Because of complexities in distribution of hardware mitigations, the timeframe will vary on a case-by-case basis,[34] and pressures may increase on stakeholders to disclose vulnerabilities. However, in the interest of protecting the public against widespread threats before mitigations are available, the CVD process should be followed and the information should be kept in confidence.

DISTINGUISHING SOFTWARE AND HARDWARE VULNERABILITIES VS. BACKDOORS

Software and hardware vulnerabilities, like other security vulnerabilities, are unintended and often result from human error or technical complexities. In contrast, backdoors are intentionally created by sophisticated cyber adversaries. A full discussion of cyber supply chain security and policy issues is outside the scope of this report. However, certain principles of coordinated vulnerability disclosure may be adapted in the context of more comprehensive supply chain risk management strategies, as determined by each organization's policy as well as legal considerations. Moreover, we recognize that mitigating backdoors presents some of the same sets of mitigation distribution challenges as unintended vulnerabilities, and therefore many of the same solutions in most cases.

Example: Mitigating Cyber Threats Related to Internet Traffic

Significant cybersecurity incidents involving internet traffic and its contents arise when traffic is harnessed for destructive ends, such as in the case of distributed denial of service (DDoS) attacks, and when traffic is improperly redirected or "hijacked" by malicious actors, such as during BGP and DNS hijacking attacks.

Four of the scenarios outlined above fall predominantly in the domains associated with mitigating threats related to the internet traffic: DDoS Botnet Attack, DDoS Server-based Attack, Border Gateway Protocol (BGP) Hijacking, and Domain Name System (DNS) Hijacking

Preventing DDoS Attacks is a shared responsibility among all stakeholders in the digital economy. In recent years, some of the most damaging DDoS attacks have involved botnets — large networks of compromised endpoints such as computers and devices — that took advantage of weak security features in Internet of Things (IoT) devices, as exemplified by the notorious Mirai botnet attack in October 2016, and have been a source of global concern ever since. And, indeed, CSDE membership includes some providers of state-of-the-art commercial DDoS mitigation services. Combating these and other automated, distributed threats has been a major goal of the CSDE, which is why in 2018 we released the *International Anti-Botnet Guide*. You can download the Guide at securingdigitaleconomy.org.

Mitigating DDoS attacks is largely handled by the Infrastructure Providers, who can act on behalf of the customers under attack. DDoS attacks are generally targeted at an end user or class of users, with the intent being to disrupt the ability of the user(s) to access their services.

In the case of mitigating DDoS attacks, the most situationally relevant player will be the underlying service provider for the user being attacked, but DDoS resolution brings in other infrastructure such as (1) the infrastructure provider of the originating attacker, (2) hosting providers/data centers, (3) content delivery networks, and (4) the multiple providers of infrastructure upon which the attack traffic travels. While the specific infrastructure provider(s) implicated in the DDoS event cannot be anticipated in advance, the Tier 1 backbone providers are minimally in a support role.

These infrastructure providers have a variety of DDoS mitigation techniques that can be used to address the issue including (1) blackholing traffic targeted towards the IP address under attack, (2) selective blackholing, which changes the BGP routing for the targeted address so that it is only from certain parts of the internet, and (3) traffic scrubbing, where the infrastructure provider redirects traffic to the targeted IP range to a scrubbing center, which scrubs the unwanted attack traffic and returns the normal traffic. There are additional network engineering and local filtering techniques which can also be used.

While the Infrastructure Provider group does not have an organization comparable to ICASI highlighted above, the connection, interconnection and peering relationships between these infrastructure provider classes are exercised daily in addressing traffic anomalies and threats.

Issues arising from internet traffic hijacking through BGP or DNS vulnerabilities are handled in a comparable fashion. Global ICT companies, in particular internet infrastructure providers (e.g., ISPs, backbone providers, DNS providers, CDNs, and providers of cloud-based infrastructure), have a variety of assets associated with internet traffic management. When internet traffic is wrongfully redirected, there are steps these companies may be able to take to remediate the situation, depending on factors such as who owns the assets responsible for the redirection and the relationship of each company to the affected parties, among other important considerations.

Focusing on these two clusters of threats provides insights into how the ICT companies choose to collaborate with either their immediate ecosystem, their extended community, or those companies outside this community. Companies leverage their own operational response protocols in collaborative initiatives. While similar in approach, these ICT companies have developed practices and protocols optimized to meeting their needs and their customers. Nonetheless, as the number of companies supporting an event expand, each one of these companies conducts a “triage” to determine who specifically (individuals/teams) within their company will work with these external players, and it’s usually only those individuals/teams that can contribute to a “solution” that are engaged. The “contribution” of company resources into any joint effort is meant to focus on resolving the issue at hand, somewhat akin to a SWAT team, and this work is consistently done on a virtual (and not physical) basis. Once a mitigation is developed, members of the virtual SWAT team convey progress and identify potential solutions to their respective companies for concurrence. Once a course of action is decided upon, the individual companies leverage their resources to implement the solution. Consistent with a unified course of action and unified messaging, the individual companies deploy those solutions using their own protocols, processes, and personnel.

Further, as outlined in the representative examples, determining which company is situationally relevant is dependent upon the event and the circumstances of the event. This report has identified the types of companies that will likely be implicated, but the specific name of the company that might be engaged is situationally dependent. Nonetheless, given their extensive global connections, the CSDE members are likely to assist in identifying which parties are the most situationally relevant and may be able to provide some support if the capacities of the identified companies are surpassed.

While there have been no events requiring a large-scale mobilization of ICT players across the ecosystem, smaller-scale events do provide an ongoing opportunity for the Infrastructure Providers as well as the Hardware/Software providers to engage with each other. Further, the companies represented within the CSDE use high-consequence exercises such as the CyberStorm and National Level Exercises to practice recognizing who the relevant players are, contacting and coordinating with those players, and developing a joint course of action. The work among industry players will continue, and the NLE 2020 series of exercises is the next major opportunity to do so.

Throughout the course of developing this report, a number of planning factors became clear: Effective incident response requires leveraging the different skill sets of diverse players, and no standard plan or protocol will accommodate every type of crisis. As demonstrated, combating malicious internet traffic, for instance, involves vastly different strategic security considerations, operations, and procedures than mitigating component vulnerabilities. Nonetheless, when CSDE members engage in incident response activities, they aim for common objectives: protecting people, nations, and economies against the worst consequences of significant cyber incidents and decreasing the likelihood of further escalation.

06 | International Coordination

IN RECENT YEARS, policymakers throughout the world have recognized the need for international cooperation and coordination to address the growing epidemic of cyber-attacks, particularly those that can rise to the level of a catastrophe.

For example, the NSTAC report states that "[a]t the levels contemplated, any ICT mobilization truly becomes an international undertaking with global implications and consequences, given the interconnected nature of the cyber ecosystem, the global distribution of cyber ecosystem functions and capabilities, and the decentralized operations of cyber bad actors. Consequently, successful cyber response must be a multi-stakeholder, multi-jurisdictional endeavor."[35]

The European Union Agency for Network and Information Security (ENISA) stated: "The cross-border nature of threats and the associated mitigation mechanisms make it essential to focus on strong international cooperation. This requires major efforts at national level, at pan-European level and globally. There needs to be close cooperation with international partners to prevent and to respond to cyber incidents."[36]

The CSDE's membership, as stewards of a global digitally connected ecosystem, are encouraged by the increasingly widespread acknowledgement that in times of cyber crisis the ability to engage in multi-stakeholder and multi-jurisdictional collaboration is a necessity.

The Need for Global Industry Leadership. A cyber crisis requires immediate multi-jurisdictional collaboration. We cannot afford to waste time with first-time introductions when a power plant has stopped working, a financial system has been disrupted, or people lose access to healthcare services. The response in these kinds of situations must be swift and well-orchestrated.

While individual governments and enterprises take steps to protect their own systems from cyber threats, these systems are built upon the infrastructure, products and services of companies reflected within the CSDE membership. Moreover, these major ICT companies are global in nature and have experience combating a broad variety of cyber threats that spread rapidly from one jurisdiction to another.

By contrast, government and enterprise system managers have different levels of operational capability and institutional knowledge, different definitions for key concepts and terminology, and different relationships with the private sector and other relevant stakeholders — all of which can result in very delayed responses during a crisis, where time is of the essence.

Even when governments want to cooperate, they often struggle when dealing directly with foreign governmental entities due to a variety of reasons, including institutional norms, operational and legal obstacles, and lack of direct familiarity or established trusting relationships with people in other governments. Under these circumstances, leveraging the major ICT player relationships, even if their products and services are not immediately relevant, can provide connections and insights into which companies will likely be in the best position to mitigate the impacts of the specific event.

On the other hand, government authorities, like subpoena power or other investigative powers may be useful when seeking the cooperation of data center operators, foreign government officials, and other key players. Governments tend to have familiarity and established relationships with the private companies that operate in their respective jurisdictions. These companies also have key relationships with governments, private stakeholders, and other parties that can be assets during a crisis. By leveraging the private sector's distinct capabilities and relationships on a voluntary and mutually beneficial basis, governments can achieve their goal of a secure digital ecosystem through the leadership of global ICT companies.

07 | Next Steps

THE CSDE CONSIDERED the global stakeholder community when developing this voluntary guide that can be deployed across numerous jurisdictions and diverse legal environments. The CSDE's industry-led approach enables critical private sector assets to be leveraged in many parts of the world for incident response purposes.

As evidenced by the CSDE C2 Consensus on IoT Device Baseline Security, where the CSDE convened 19 associations from across the ICT sector to solve a common problem, we are well-positioned to develop operational and policy guidance that will be essential for shaping, enhancing, and promoting incident response capabilities.

By strengthening the relationships among key stakeholders, as well as developing guides to mitigate specific kinds of cyber threats and vulnerabilities, the CSDE will continue to serve as a critical forum for cyber policy leaders representing global ICT companies that are on the front lines during cyber-attacks and are committed to securing the digital economy.

08 | Appendix A: Cyber Crisis Scenarios Examined by CSDE

THE FOLLOWING SCENARIOS involve categories of cyber crises that could rise to the level of major disruptions of the global internet and communications ecosystem. These scenarios were chosen by CSDE members in close coordination with industry and government stakeholders.

- **DDoS Botnet Attack** — Malware infects a large number of devices to create a massive botnet and launch DDoS attacks against high value targets.
- **DDoS Server-based Attack** — An attacker exploits the vulnerabilities in servers to launch hugely amplified DDoS attacks.
- **Border Gateway Protocol (BGP) Hijacking** — A BGP hijacking attack wrongfully redirects internet traffic and may cause disruptions to websites and online services while also enabling attackers to steal data, conduct espionage, and perpetrate other abuses.
- **Domain Name System (DNS) Hijacking** — Malicious actors alter information on a DNS server to redirect internet traffic to the wrong online destination, such as a fraudulent website that misleads the public.
- **Software Vulnerabilities: Open Source** — Malicious actors discover security vulnerabilities in open source software components, which are used in commercial applications that proliferate widely throughout the internet ecosystem.
- **Software Vulnerabilities: Zero-Day** — Malicious actors discover software zero-day security vulnerabilities — vulnerabilities that software developers do not know about — and write exploit codes to gain unauthorized control and impair the functions of information systems all over the world.
- **Hardware Vulnerabilities: Processor Architectures** — A processor manufacturer identifies and discloses a vulnerability to a restricted set of ecosystem partners whose involvement in the coordination efforts is necessary for the vulnerability mitigation development and validation efforts.
- **Injection of Malicious Code in Software and Hardware Components** — A state-sponsored bad actor manages to insert malicious code into the software or hardware of major ICT companies, compromising systems in industry and/or government. The malicious code enables cyberespionage operations against the organizations whose systems are compromised.
- **Destructive Malware** — Sophisticated malware targets and destroys important data or prevents the system from booting successfully, rendering it unusable.
- **Ransomware —** Profit-seeking criminals target information systems with crucial data, such as computers used by governments, businesses, and even hospitals.
- **Advanced Persistent Threat (APT): Industrial Systems** — A nation state or well-financed, highly sophisticated actor develops malware that targets industrial control systems.
- **Cloud Provider Compromise** — A cyber-attack against a major cloud services provider, possibly a supply chain attack, gives malicious actors the ability to target the provider's clients, which may include industry and government, causing significant economic damage or compromising national security.

DDoS Botnet Attack

Malware infects a large number of devices to create a massive botnet and launch DDoS attacks against high value targets. The botnet may span dozens of countries and require significant international coordination to mitigate.

Mirai Botnet

On October 21, 2016, the Mirai Botnet targeted Dyn, a major DNS provider, with a wave of large distributed denial of service (DDoS) attacks.[37] A second attack struck two hours later, and this time customers could not access the websites of Dyn's customers such as Twitter, Netflix, Reddit, CNN, PayPal, and Spotify.[38] The botnet used to coordinate this attack was comprised of thousands of vulnerable devices such as CCTV cameras, which together fired 1.2 terabytes of data on Dyn, shutting down several large websites.[39] The scale and severity of the Mirai Botnet attack demonstrated the vulnerabilities within the global digital ecosystem and the growing threat that DDoS attacks pose to our businesses and organizations.

Evolution of IoT Botnets

Since 2016, new attack vectors and delivery methods have been found that make botnets an even more serious hazard. For example, in January 2018, three large DDoS attacks were launched at several financial institutions, all built off the Mirai Botnet's source code.[40] Since then, the Mirai botnet's code has been publicly released.[41] So now criminals in different parts of the world can experiment and create their own variants of IoT botnets. Strategies that would have worked against Mirai will not necessarily work against newer botnets.[42]

For example, Mirai needed default passwords to gain control of devices. Newer botnets like Satori — which generated about 280,000 bots within 12 hours — Wicked, and Reaper have found ways around this weakness.[43] Because of the evolution of IoT botnets, many devices that would have been impervious to Mirai may end up becoming part of a botnet today.

To make matters worse, some of the new botnets can be rented for a low fee by cyber-criminals who lack the technical skills to make a botnet of their own. This arrangement, called malware-as-a-service (MaaS), expands the threat landscape to a broader set of bad actors.[44]

In early 2019, a Liberian telecom company became the subject of a lawsuit after hiring a criminal hacker to launch DDoS attacks against a rival to gain an unfair competitive advantage.[45] The hacker used a custom botnet based on Mirai and rented infected security cameras and routers from other hackers.[46] At their peak, the attacks disabled access for *most internet users in the country*, further adding to global concerns about IoT security.[47]

DDoS Server-based Attack

An attacker exploits the vulnerabilities in memcached servers to launch hugely amplified DDoS attacks. Because memcached servers — often used in cloud computing and Linux operating systems — do not require authentication, an attacker can falsify ("spoof") the IP address of the computer contacting the servers. Most of the memcached servers belong to business enterprises and other organizations for which security is not a primary concern. By tricking a handful of servers into targeting a single fake address, an attacker can amplify the power of an attack thousands of times. Memcached server-based attacks currently hold the world record for largest DDoS attacks.

Vulnerable Memcached Servers

On the first of March, 2018, the cloud service provider Akamai revealed that its client, GitHub, had been targeted by a DDoS attack measuring in at 1.3 Tbps.[48] This was the largest publicly recorded DDoS attack at the time.[49] The attack exploited a vulnerability in memcached servers — which are found mostly in cloud environments and communicate using protocols that operate without authentication, allowing pretty much anyone to request data from them.[50] According to Cloudflare, memcached servers respond with packets up to 51,000 times larger than the packets they receive. This allows attackers to coordinate much larger attacks using very little effort.[51]

Akamai was able to defend GitHub successfully using a number of mitigations strategies.[52] A few days later, however, an even bigger 1.7 Tbps DDoS attack targeted another service provider.[53] Such developments demonstrate how innovations in attack methods are being used to amplify DDoS attacks, testing the limits of providers' capabilities.

In January 2019, a memcached attack was discovered to exceed 500 million packets per second (mpps), which is approximately four times the volume of the previous year's attack on GitHub.[54] Since then, similarly high-volume attacks have been seen. While these attacks are not as large in terms of bandwidth as the record-setting 2018 attacks, the increase in attack volume is troubling because the sheer number of packets can exhaust network resources and can do as much damage as larger attacks.[55] A barrage of small attacks can also be used to mask deeper, more serious intrusions by avoiding detection while attackers gain foothold within compromised systems.[56]

Border Gateway Protocol (BGP) Hijacking

A BGP hijacking attack wrongfully redirects internet traffic and may cause disruptions to websites and online services while also enabling attackers to steal data, conduct espionage, and perpetrate other abuses. Sometimes, however, wrongful re-routing of IP addresses is a consequence of human error. Investigators may find it challenging to determine whether the hijacking was intentional and whether sensitive information was compromised.

As a technique in the arsenal of bad actors, BGP hijacking has been used to target finance websites (e.g., Master Card, Visa) and cryptocurrency websites, among many other kinds of sites. Even more troublingly, in the hands of nation-states with adversarial goals, BGP hijacking may be perceived as a precursor to cyberwarfare and undermine confidence in the security of the interoperable internet ecosystem.[58]

China Absorbs 15% of World's Internet Traffic in 2010

In 2010, bad instructions issued by Chinese telecom companies routed traffic from multiple countries through Chinese servers — absorbing 15% of the global internet's traffic.[59] While the whole incident lasted less than 20 minutes, governments throughout the world took notice — in no small part because many websites with .gov and .mil domains were disrupted, including those belonging to the U.S. Senate and various branches of the military.[60] Some of the world's leading technology companies were also affected.[61]

The US-China Economic and Security Review Commission stated that "the Commission has no way to determine what, if anything, Chinese telecommunications firms did to the hijacked data" and "incidents of this nature could have a number of serious implications."[62]

2017 Russian Telecom Incidents

In April 2017, a Russian controlled telecom seized control of traffic from two dozen financial services companies, including Visa and MasterCard.[63] Security experts noted that the incident was suspicious because normally accidental leaks absorb more traffic and are not limited to specific industries.[64] A few months later, in December 2017, major technology companies including Google, Facebook, Apple, and Microsoft discovered their traffic was being routed to a previously unheard of Russian internet service provider, again raising strong suspicions among the security community.[65]

2018 Google Incident

In November 2018, Google was revealed as the victim of a major BGP hijack — the worst in the company's history — targeting a broad array of services. Initial reports suggested that the attack, which has been traced to servers in Russia, China, and Nigeria (including servers of state-owned telecom companies) amounted to a "wargame experiment" and may be a prelude to even more severe attacks in the future.[66] Subsequent reports have pushed back against this account, explaining that the incident was caused by an erroneous BGP configuration of an ISP in Nigeria.[67] But as an article in *Forbes* points out, "If China isn't hijacking Internet traffic, there's no reason why not."[68] The fact is that our current systems were built on trust and are exploitable by bad actors.

Domain Name System (DNS) Hijacking

Malicious actors alter information on a DNS server to redirect internet traffic to the wrong online destination, such as a fraudulent website that misleads the public. A fraudulent website may convincingly impersonate a well-known financial institution, government agency, or social media platform to deceive users into disclosing sensitive information (social security numbers, credit card numbers, passwords, etc.) It may also install various types of malware on user devices. Typically, if users know they correctly typed the URL of a legitimate website, they will not question its authenticity.

One of the dangers of DNS hijacking is that misinformation can spread rapidly from one DNS server to another, creating an international incident.[69] Accidents involving DNS root server instructions have shown us what such a scenario looks like,[70] and more recent events prove the validity of longstanding concerns about exploitation of DNS vulnerabilities for cyber-espionage.[71]

2010 Chinese DNS Root Server Incident

In 2010, a Chilean ISP mistook DNS instructions from a root server in China — where certain websites cannot be accessed as a matter of national policy — with instructions meant for other parts of the world.[72] Neighboring ISPs trusted and shared the information provided by their peer.[73] Before long, the error spread all way to the United States. The consequences of this mistake became apparent to American users as they suddenly lost access to popular websites that are banned in China such as YouTube, Twitter, and Facebook.[74]

What is noteworthy about this incident from a security perspective is *how* the wrong DNS information spread. China purposely alters the instructions on its own root servers.[75] If a user in China types the URL of a prohibited website into a browser, they will not be able to access the destination associated with that URL because the DNS configuration takes them elsewhere: a government-controlled server.[76]

What this accident shows, therefore, is that users across the world can find themselves redirected to servers of a government that does not abide by international norms and exploits DNS vulnerabilities to conduct cyber-espionage, and the users may not even notice.[77]

2019 DNS Hijacking Campaign

In January 2019, FireEye reported that hackers with apparent ties to the Iranian government have engaged in massive DNS hijacking on a global scale to divert sensitive information from proper destinations into the custody of malicious actors.[78]

Stolen sensitive information included login credentials and non-public data from a variety of stakeholders in the global ICT ecosystem, including ISPs, government entities, and organizations in various continents: North America as well as North Africa, Europe, and the Middle East.[79]

The specific targets and category of data stolen match the Iranian governments' strategic interests.[80] Now that the bad actors have this data, they will be able to launch continuous cyber-attacks for years to come.[81] Security experts warn that this was just the first step in a bigger plan.

Software Vulnerabilities: Open Source

Malicious actors discover security vulnerabilities in open source software components, which are used in commercial applications that proliferate widely throughout the internet ecosystem. Open source vulnerabilities are a key point of discussion in supply chain risk management.

Any discussion about open source vulnerabilities must start with the acknowledgement that there are many advantages to open source software, as evidenced by the degree of proliferation.[82] More than 95% of commercial applications today use some open source components and, on average, the open source components make up a third of the application's code.[83] The question is: In the absence of a specific developer to whom a software component can be directly attributed, how should the ICT stakeholder community work together to mitigate open source vulnerabilities?

Equifax Data Breach and Follow-up

In mid-May 2017, hackers exploited vulnerable open source code in Equifax web applications to steal social security numbers and other private information of 148 million people.[84] The code was known to be vulnerable for several months at the time when the breach occurred — yet the credit agency, like many other companies, did not act quickly enough to prevent data theft.[85]

The bigger ecosystem-wide problem is that Equifax is not alone. Currently, thousands of organizations download and use software known to be vulnerable, including the unpatched software that resulted in the theft of 148 million people's data.[86] In fact, only about one in five companies making use of the software have taken corrective measures after the breach.[87]

There are reasons for this: In the current state of the ecosystem, rapidly patching open source software components remains a challenge for many companies.[88] Part of the problem is that open source patches are sometimes difficult to update and a variety of technical difficulties prevent companies from being able to do so regularly.[89]

However, efforts are already underway within the ICT stakeholder community to collectively address this problem through market-based solutions and transparency measures.[90] These measures are being discussed in a variety of multi-stakeholder and partnership venues.[91]

Software Vulnerabilities: Zero Day

Malicious actors discover software zero day security vulnerabilities — vulnerabilities that software developers do not know about — and write exploit codes to gain unauthorized control and impair the functions of information systems all over the world. These can include corporate or government information systems containing highly sensitive information.

The goal here is not to shame any particular company, but rather to identify ways that ICT companies can work together to spread information about security vulnerabilities when they affect the whole ecosystem and facilitate ecosystem-wide solutions. No matter how much a company invests in top coding talent and follows secure-by-design best practices, human mistakes in code will inevitably arise from time to time.

Examples of Zero Day Vulnerabilities

Bad actors often fall back onto zero-day exploits to execute their malicious codes. The exploits may be found in common products that millions of people use. For example, the exploit called CVE-2017-0199 abuses a logic flaw in Microsoft Word and fetches a remote resource from the internet — a malicious payload that attackers host online.[92] A substantially similar exploit is CVE-2018-9174, which leverages the library used by Internet Explorer to render web pages and ultimately download a payload on the victim's computer.[93] Even though Microsoft devotes significant resources to patching vulnerabilities, many of these threats can remain dangerous if businesses or individuals fall behind on updating their software.[94] Therefore, end-user awareness can be the difference between successfully securing the ecosystem against an exploit.

Zero day vulnerabilities are not merely an inconvenience to consumers — they can give rise to grave national security concerns. For example, it appears that in 2018 the Sejong Institute, a South Korean think tank that conducts national security research and holds large amounts of strategically important data, was attacked by hackers ostensibly from North Korea.[95] They accomplished this attack by exploiting a zero day vulnerability in Active X software.[96]

Zero Day Vulnerability Disclosure

Government agencies in charge of cybersecurity, for example the United States' NSA, have two often-irreconcilable interests when it comes to zero day vulnerabilities. They want to protect their own country and allies from preventable cyber-attacks.[97] On the other hand, by keeping zero day vulnerabilities secret, they gain a valuable instrument for disrupting opponents.[98] Because of these irreconcilable incentives, the government may or may not disclose security vulnerabilities.[99] The decision will be made situationally.

In general, global ICT leaders will patch vulnerabilities when they are discovered to be affecting consumers, provided the software is still supported. However, not all companies are subject to the same market forces or other external pressures. Some companies may be influenced by relationships with governments or other third parties. As global ICT leaders address the issue of zero day vulnerabilities, it is necessary to be open-eyed to the reality that not all players will always be motivated to maximize pre-incident protective capabilities through disclosure.

Hardware Vulnerabilities: Processor Architectures

A processor manufacturer identifies and discloses a vulnerability to a restricted set of ecosystem partners whose involvement in the coordination efforts is necessary for the vulnerability mitigation development and validation efforts. The manufacturer identifies mitigations, delivered through patches to microcode/firmware, operating system, and other system software, as needed. Validation, distribution, and installation of the mitigation often requires a multi-party coordinated vulnerability disclosure process, coordinated by the processor manufacturer.

Spectre and Meltdown

The hardware vulnerabilities Spectre and Meltdown, disclosed in January 2018, took advantage of a feature called speculative execution common to most modern processor architectures.[100] The Spectre and Meltdown Proofs of Concept demonstrated the possibility of malicious actors using specific, targeted malware to infer data values that would normally be protected without proper authorization (for example sensitive data such as passwords). Thus, the great task of developing, testing, and deploying mitigations for these vulnerabilities in multi-party CVD settings has been a priority for industry.

Currently, there are no known instances of these vulnerabilities being exploited, and taking advantage of the vulnerabilities is difficult — a process that would require significant skill, planning, and investment.[101]

Spectre and Meltdown do, however, serve to illustrate some of the complexities inherent in responding to hardware vulnerabilities and distinct from most software vulnerabilities: (1) the number of parties that must coordinate is often greater in the hardware context, making coordination more difficult, and often more time-consuming due to that complexity;[102] (2) mitigations may involve multiple layers of the affected systems, not just

the hardware layer — a number of companies have released software patches that work around the problems caused by Spectre and Meltdown, including patches to microcode, firmware, operating systems, or other software (this requires coordination between and among multiple parties, led principally by the hardware vendor);[103] (3) distributing mitigations may involve parties other than the vendors themselves to develop, test and deliver the mitigations to end users, keeping information concerning these vulnerabilities in confidence while doing so.[104]

Notwithstanding these substantial challenges, there has been unprecedent coordination across ICT segments to address these kinds of vulnerabilities, and as processes continue to be refined mitigation efforts will benefit accordingly.

Injection of Malicious Code in Software and Hardware Components

A state-sponsored bad actor manages to insert malicious code into the software or hardware of major ICT companies, compromising systems in industry and/or government. The malicious code enables cyberespionage operations against the organizations whose systems are compromised.

Component Backdoors

In recent years, policymakers have focused on the possibility of specific nation-states and bad actors inserting backdoors into ICT components manufactured overseas.[105] This is a complex issue as it may involve matters of supply chains, international trade, and economics — a full discussion of the policy implications is beyond the scope of this report.

In the past decade, even the NSA, an agency that protects critical U.S. security interests, may have faced serious challenges related to component backdoors.[106] This problem may have the potential to afflict industry as well.[107] For example, while the allegations of a 2018 *Bloomberg* report that China has inserted hardware backdoors into the supply chains of American companies have been strongly denied or met with strong skepticism by many segments of industry — including the companies whose supply chains would have been theoretically compromised — many experts in government, industry, and civil society nonetheless worry that such a feat is not technologically infeasible.[108] As such, the CSDE should discuss how the risk of injection of malicious code fits into its potentially broader engagement with issues of supply chain risk management.

Destructive Malware

Sophisticated malware targets and destroys important data or prevents the system from booting successfully, rendering it unusable. This malware can spread through the typical channels by which malware spreads. Once it infects a system, the malware's execution can be triggered remotely by an attacker's command or the malware can activate automatically after a defined amount of time.

Malware with destructive capabilities comes in many forms and may have other features besides wiping data or rendering system assets unusable. For example, nation states have combined destructive malware with ransomware to obfuscate their motives, and Advanced Persistent Threat (APT) groups have covered their tracks by destroying digital evidence.[109]

One of the major challenges associated with destructive malware is the speed of execution. Often, by the time somebody discovers the malware's presence, it is already too late to defend the system or its data.[110] Because destructive malware can typically target the backup data on an infected system, storing backup data elsewhere is essential to recovery efforts.[111] The degree of destructive capability and the amount of data destroyed will vary depending on the specific techniques used to damage files or systems.[112]

Shamoon

Shamoon malware emerged in 2012 when politically motivated hackers targeted oil and gas companies in the Middle East.[113] The most notable target was Saudi Aramco — Shamoon disabled 30,000 of the company's workstations for nearly a month.[114] As a result of this cyber-attack, Saudi Aramco's ability to supply 10% of the global oil supply was put at risk.[115]

In 2016, Shamoon re-emerged and targeted petrochemical companies, as well as the Saudi central bank system.[116] This second version of the malware was considered a threat to mission-critical computers of targeted organizations.[117]

The latest version of Shamoon, which emerged in 2018, is even more destructive than its predecessors.[118] This is because it comes paired with a second piece of malware called Trojan.Filerase, which overwrites files on a computer while Shamoon itself targets the Master Boot Record (MBR), the part of a hard disk that provides information necessary to load the operating system.[119]

BlackEnergy and GreyEnergy

In December 2015, in the middle of winter, about 230,000 people in Ukraine lost power for six hours after a devastating cyber-attack on electricity distribution companies; the destructive malware used by the attackers is known as BlackEnergy.[120] This was the first widely recorded successful cyber-attack on an electrical grid, and experts worry it could be applied to many other critical systems, including hospitals.[121]

In October 2018, researchers at ESET released a whitepaper on GreyEnergy, a successor to Black Energy that targets critical infrastructure networks in Central and Eastern Europe.[122] This newer destructive malware remains a clear and present danger in the ecosystem.

Wiper Ransomware

Destructive malware has often been associated with ransomware attacks, even though deleting ransomed data has generally fallen out of favor among profit-seeking criminals. As Symantec explains, "you cannot easily monetize a computer that has been destroyed."[123]

In 2017, malware called NotPetya — a highly sophisticated cyber-attack disguised as ransomware — wreaked havoc across Europe, Asia, and the Americas.[124] The malware was unleashed by a nation state for the purpose of damaging specific systems and wiping out records with military precision, ensuring that the data cannot be recovered.[125] Altogether, the destruction from NotPetya resulted in over $10 billions of damage, making it the costliest cyber-attack in history.[126]

Later the same year, in Japan, an extensive hacking campaign that exploited leaked NSA technology targeted the systems of companies across multiple industries; the attackers deployed destructive malware called ONI to cover their tracks.[127] While not as costly as NotPetya, this incident and others like it show that wiper ransomware is a growing trend.[128]

By combining destructive malware with ransomware, nation states and other sophisticated actors can sometimes succeed at making their intentions impenetrable to expert analysts.[129]

Olympic Destroyer

The opening ceremony of the 2018 Winter Olympics was disrupted by destructive malware called Olympic Destroyer. The malware was deployed in a cyber-attack that affected attendance — people could not print out their reservations — and coverage of the ceremony — the malware disabled internet access and telecasts, rendered drones unusable, and shut down the official Pyeongchang 2018 website.[130] Cisco's Talos security division concluded that because the malware wiped "all available methods of recovery" its purpose was destructive in nature.[131]

VPNFilter

In May 2018, Cisco's Talos security division issued an alert about VPNFilter, stealthy and highly versatile malware that has infected about a half-million home and small business routers.[132] While this malware currently serves an espionage function, researchers have determined it has worrisome destructive capabilities.[133] Part of the VPNFilter code is shared in common with BlackEnergy, the malware that caused power outages in Ukraine by attacking electricity distribution companies.[134] Most of the routers infected with VPNFilter are in Ukraine, and experts warn the malware may cause disruptions to targeted infrastructure.[135]

Ransomware

Profit-seeking criminals target information systems with crucial data, such as computers used by governments, businesses, and even hospitals. The criminals use malware that encrypts files on the infected systems, denying legitimate users access. A message then appears demanding payment in exchange for restored access. The proliferation of ransomware has been facilitated by ransomware-as-a-service (RaaS), which is when cybercriminals make malicious code available to less tech-savvy bad actors in exchange for agreed-upon compensation.

NOTE: In some cases, bad actors may disguise destructive cyber-attacks as ransomware. In these cases, the data may be impossible to recover even if victims are willing to pay the ransom.

Atlanta/WannaCry/Ransomware-as-a-Service

Ransomware first emerged in Eastern Europe nearly a decade ago, when criminals locked up computers with malicious code and demanded payment in return for their restoration.[136] Since then ransomware has become much more prevalent and complex. It is used by profit-seeking individual hackers and sophisticated criminal organizations alike — they often demand virtual payment in the form of cryptocurrencies such as bitcoin.[137] In 2016, cybersecurity experts estimated that criminals reaped over $1 billion in ransom payments using this attack method.[138] Attackers usually target organizations where downtime is not an option, such as in hospitals or

financial institutions.[139]

In 2018, the City of Atlanta was targeted by a sustained attack that demanded $51,000 in return for the restoration of their computer network systems.[140] During this attack Atlanta's police officers were forced to write reports by hand, the court was unable to validate warrants, and the city stopped taking employment applications.[141]

Another severe series of attacks were orchestrated by a North Korean linked hacker group called Lazarus.[142] They produced a malware called "WannaCry" which crippled systems around the world that used Windows XP.[143]

A frightening development in the world of ransomware has been "Ransomware-as-a-Service".[144] This allows criminals lacking sophisticated technical knowledge the ability to commit effective attacks with the help of pre-made toolkits found in marketplaces on the Dark Web.[145] This phenomenon has promoted the creation and spread of thousands of different types and strains of ransomware, making remediation and attribution very challenging for those trying to fight this malware.[146]

NotPetya Ransomware Attacks

The NotPetya "ransomware" was born of a massive cyber-attack against Ukrainian institutions in 2017, allegedly by the Russian military.[147] The attack came cleverly disguised as ransomware of the type used by criminals to make a profit, in order to conceal the attacker's motive: damage to specific systems.[148] In specific cases, rather than encrypting data to ransom for payment, NotPetya wiped out computers' deep-seated records, ensuring that recovery of data was impossible.[149] To make matters worse, NotPetya did not stay contained to a single country. Before long, it spread across Europe, Asia, and the Americas — causing more than $10 billion damages globally.[150]

The NotPetya outbreak was possible because of supply chain vulnerabilities, thereby raising concerns in the global stakeholder community about the trustworthiness of particular companies and the relationships between companies and particular governments.[151]

Geographic Restrictions on Ransomware

Ransomware attacks have infected machines all over the world, including machines in the countries where the ransomware originated.[152] Some of the more sophisticated modern ransomware only targets specific countries, or rather it is programmed not to target machines in specific countries.[153]

The Anatova ransomware discovered in early 2019 is a perfect example.[154] This advanced malware will not attack machines based in Russia and other CIS countries, as well as Egypt, India, Iraq Morocco, and Syria.[155] Many of the victims have been based in the United States.[156]

Advanced Persistent Threat (APT): Industrial Systems

A nation state or well-financed, highly sophisticated actor develops malware that targets industrial control systems. The malware may spread via means that do not require an internet connection (e.g., USB ports). The malware may infect computers in many different countries, looking for a strategically important target. When the malware finds the target, it can disrupt normal operations and result in severe damage.

Saudi Petrochemical Plant

In August 2017, a Saudi petrochemical company was the victim of a cyber-attack that could have been lethal.[157] Experts believe the purpose of the attack was not merely the incapacitation of industrial systems but rather to trigger an explosion that could result in loss of human life.[158] The only reason an explosion did not take place is because of a computer coding error on the attackers' behalf.[159] Experts worry that similar attacks could take place in the future, possibly using similar exploits.[160]

Global Nature of the Threat

The sophisticated bad actors behind Trisis malware, which was used in the 2017 attack on a Saudi petrochemical company, have expanded their operations globally.[161] FireEye's research links the hacking group to Russia, specifically a lab in Moscow.[162] Multiple U.S. companies are among the targets of this group's cyber-attacks.[163] U.S. officials have publicly confirmed that hackers attempted to breach industrial control systems of firms that operate on US soil — this would enable the hackers to cause life-threatening damage.[164]

Details about attempted breaches of industrial systems cannot always be made public — for example, the names of companies breached, the number of companies breached, technical details of the breaches, and severity of threats to critical infrastructure may be withheld. However, it is clear that the government wants companies operating in the United States and elsewhere to be on high alert against APTs.[165] A common tactic for hackers is to compromise IT systems that have relatively low security, in order to gain a tactical foothold, before launching attacks aimed at more secure systems.[166]

APT10/Chinese Cyber-Espionage

In December 2018, the U.S. government attributed attacks carried out by the cyber-espionage group commonly known as APT10 — also known as Red Apollo, Stone Panda, CVNX, Potassium, and MenuPass — to the Chinese Ministry of State Security (MSS).[167] Known to be active since at least 2009, the APT10 group has targeted information that would be useful to the Chinese state during trade negotiations, as well as other high value intelligence assets.[168]

In particular, APT10 has targeted commercial entities of strategic interest to China including, according to FireEye's profile, companies involved in construction, engineering, aerospace, telecom and government.[169] APT10 has been notably active in the United States, Europe, and Japan. Recent APT10 targets include global managed service providers, such as IBM and Hewlett Packard Enterprise, and possibly other targets we do not yet know about.[170]

Cloud Provider Compromise

A cyber-attack against a major cloud services provider, possibly a supply chain attack, gives malicious actors the ability to target the provider's clients, which may include industry and government, causing significant economic damage or compromising national security.

The cloud has undeniable benefits for organizations all over the world, including businesses and governments. With increased reliance on cloud services comes the need to secure unique attack surfaces in the cloud environment, including providers' own systems — to protect their clients' sensitive information of interest to bad actors.

Operation Cloud Hopper

The hacking group APT10, whose actions the United States has attributed to the Chinese government, carried out an extensive cyber-espionage campaign that began in 2014 and was not discovered until 2017.[171] Known as Operation Cloud Hopper, the campaign targeted managed service providers to infect their client companies with malware.[172] APT10 conducted this malicious series of attacks across fifteen countries in different regions of the world, including the United States and key allies.[173] According to experts at multiple security research groups, the Chinese hackers' targeting of managed service providers demonstrates their espionage tactics have evolved and accentuates the importance of addressing supply chain risks.[174]

Cloudborne

On February 26, 2019, security experts at Eclypsium Inc. revealed information about a cloud-based vulnerability known as Cloudborne.[175] The vulnerability could theoretically enable hackers to exploit components found in server motherboards that major cloud providers use in data centers.[176] According to the security experts at Eclypsium Inc., hackers can implant malware into the server's firmware or create a backdoor to steal data from the provider's clients.[177]

Possibility of Massive Economic Damages

According to the Ponemon Institute's 2017 Cost of Data Breach Study, the average data breach costs about $3.62 million.[178] While this damage can be an enormous setback for an individual company — and the aggregate costs of such breaches are significant for the global economy — the average data breach will not generally rise to the level of a national security concern, unless the data stolen was of a particular nature.[179] On the other hand, the damage of a cyber-attack against a major cloud service provider could become a matter of national or global concern due not only to the type of data stolen but also because of the financial impact.[180] An attack against a cloud service provider could cause tens of billions of dollars in damage, with the highest estimate around $120 billion in damages[181] —$110 billion more than the costliest cyber-attack that has actually taken place and about a fifth of one percent of global GDP.[182]

To put this in further perspective, the damage from Superstorm Sandy was about $70 billion[183] and the damage from Hurricane Katrina was about $105 billion.[184] Which means a cyber-attack against a cloud service provider could be far more damaging economically than some of the worst natural disasters — and the attack could be about *twelve times* as damaging as the costliest cyber-attack in history.[185] It is essential, therefore, that we are well-positioned to coordinate as stakeholders to reduce the effectiveness of bad actors and mitigate against these kinds of worst-case scenarios.

09 | Endnotes

1 *See generally* Appendix A.

2 *See* FIRST, PSIRT Services Framework (2018), *available at* https://www.first.org/education/FIRST_PSIRT_Service_Framework_v1.0. *See also* international standards on coordinated vulnerability disclosure and handling processes, ISO/IEC 30111 (2013) (in renewal stages, 2019) and ISO/IEC 29147 (2018).

3 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

4 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.

5 Danny Palmer, *Cloud computing: Why a Major Cyber-Attack Could Be as Costly as a Hurricane*, ZDNET (Jan. 17, 2018), https://www.zdnet.com/article/cloud-computing-why-a-major-cyber-attack-could-be-as-costly-as-a-hurricane.

6 *See generally* Appendix A.

7 Adam Vincent, *BlackEnergy Malware: How Hackers May Tackle our Infrastructure*, INFOSECURITY (Feb. 7, 2018), https://www.infosecurity-magazine.com/opinions/blackenergy-malware-infrastructure.

8 Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

9 Andy Greenberg, *The White House Blames Russia for NotPetya, the "Most Costly Cyber Attack in History"*, WIRED (Feb. 15, 2018), https://www.wired.com/story/white-house-russia-notpetya-attribution.

10 *See, e.g.*, Patel, *BlackEnergy, Grid-Disrupting Malware, Has a Successor, Researchers Warn*, POWER (Oct. 18, 2018), https://www.powermag.com/blackenergy-grid-disrupting-malware-has-a-successor-researchers-warn/?pagenum=1.

11 *See, e.g.*, Andy Greenberg, T*he Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

12 Nat'l Sec. Telecomm. Advisory Comm., NSTAC Report to the President on Internet and Communications Mobilization 12 (Nov. 16, 2017) [hereinafter NSTAC Report], *available at* https://www.dhs.gov/sites/default/files/publications/NSTAC%20-%20Information%20and%20Communications%20Technology%20Mobilization%20Report%2011-19-2014.pdf.

13 Homeland Security Advisory Council, *Final Report of the Cybersecurity Subcommittee on Incident Response*, DEP'T OF HOMELAND SEC. (June 2016), https://www.dhs.gov/sites/default/files/publications/HSAC_Cybersecurity_IR_FINAL_Report.pdf.

14 *See, e.g.*, ENISA, *Strategies for Incident Response and Cyber Crisis Cooperation* (Aug. 25, 2016), https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation.

15 TechTarget, Network Operations Center, https://searchnetworking.techtarget.com/definition/network-operations-center (last accessed May 14, 2019).

16 NIST, Cybersecurity Framework, https://www.nist.gov/cyberframework (last accessed May 14, 2019).

17 *See* FIRST, PSIRT Services Framework v.1.0 (2018), *available at* https://www.first.org/education/FIRST_PSIRT_Service_Framework_v1.0.

18 yberSeek, Cybersecurity Career Pathway, https://www.cyberseek.org/pathway.html (last accessed May 14, 2019).

19 *Id.*

20 See ITU, Cybersecurity Information Exchange Techniques, https://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/cybex.aspx (last accessed June 9, 2018).

21 The ability of the private sector (e.g., ISACs) to aggregate and correlate like incidents is considered foundational to cyber awareness and the creation of a common operating framework." NSTAC Report, supra note 10.

22 *See generally* Better Business Bureau, State of Cybersecurity Among Small Businesses in North America (2017), *available at* https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf.

23 ENISA., Information Sharing and Analysis Centers, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing (last accessed June 9, 2018).

24 NSTAC Report, supra note 10, at 21.

25 *Id.*

26 *Id.*

27

28 *See, e.g.*, Statement from the Industry Consortium for Advancement of Security on the Internet (ICASI) on the Bluetooth BR/EDR Vulnerability (Aug. 13 2019), https://www.icasi.org/br-edr-encryption-key-bluetooth-vulnerability/addressing a Bluetooth protocol vulnerability, CVE-2019-9506.

29 *See* international standards on coordinated vulnerability disclosure and handling processes, ISO/IEC 30111 (2013) (in renewal stages, 2019) and ISO/IEC 29147 (2018). *See also* ENISA, ENISA REPORT ON GOOD PRACTICE GUIDE ON VULNERABILITY DISCLOSURE: FROM CHALLENGES TO RECOMMENDATIONS (2016), at 9 ("The global nature of the internet requires a more transnational approach to the topic of vulnerability disclosure"), *available at* https://www.enisa.europa.eu/publications/vulnerability-disclosure.

30 *Id.* International standards on coordinated vulnerability disclosure and handling processes, ISO/IEC 30111 (2013) (in renewal stages, 2019) and ISO/IEC 29147 (2018). *See also* THE CENTER FOR CYBERSECURITY POLICY AND LAW, IMPROVING HARDWARE COMPONENT VULNERABILITY DISCLOSURE (2019), https://centerforcybersecuritypolicy.org/improving-hardware-component-vulnerability-disclosure for a discussion on Multi-Party CVD in the context of hardware.

31 NIST, Cybersecurity Framework, RS.AN-5, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last accessed June 29, 2019).

32 FIRST, Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure (2017), *available at* https://www.first.org/education/FIRST_PSIRT_Service_Framework_v1.0.

33 THE CENTER FOR CYBERSECURITY POLICY AND LAW, IMPROVING HARDWARE COMPONENT VULNERABILITY DISCLOSURE (2019) 3, https://centerforcybersecuritypolicy.org/improving-hardware-component-vulnerability-disclosure.

34 *See also* the discussion on this issue in DIGITAL EUROPE, JOINT INDUSTRY LETTER ON CYBERSECURITY VULNERABILITIES ADMINISTRATIVE REGULATION RESPONSE TO MIIT PUBLISHED DRAFT FOR COMMENTS (July 18, 2019), https://www.digitaleurope.org/resources/joint-industry-letter-on-cybersecurity-vulnerabilities-administrative-regulation-response-to-miit-published-draft-for-comments/.

34 *Id.*

35 NSTAC Report, *supra* note 10, at 21.at ES—3.

36 ENISA, EU Cyber Cooperation: The Digital Frontline (2012), *available at* https://www.enisa.europa.eu/publications/eu-cyber-cooperation-the-digital-frontline.

37 Ben Bours, *How a Dorm Room Minecraft Scam Brought Down the Internet*, WIRED (Dec. 13, 2017), https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet (reporting that a botnet experts feared "might be the work of a nation-state practicing for an attack" was revealed as the handiwork of a 21-year-old college student and his friends).

38 Brad Chacos, *Major DDoS Attack on Dyn DNS Knocks Spotify, Twitter, Github, PayPal, and More Offline*, PC WORLD (Oct. 21, 2016), https://www.pcworld.com/article/3133847/ddos-attack-on-dyn-knocks-spotify-twitter-github-etsy-and-more-offline.html; *See also* Nicky Woolf, *DDoS Attack that Disrupted Internet was Largest of its Kind in History, Experts Say*, THE GUARDIAN (Oct. 26, 2016), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

39 Chris Bing, *You can Now Buy a Mirai-Powered Botnet on the Dark Web*, CYBERSECOOP (Oct. 27, 2016), https://www.cyberscoop.com/mirai-botnet-for-sale-ddos-dark-web.

40 Zack Whittaker, *A New Mirai-Style Botnet Is Targeting the Financial Sector*, ZDNET (April 5, 2018), https://www.zdnet.com/article/new-mirai-style-botnet-targets-the-financial-sector.

41 Brian Krebs, Source Code for IoT Botnet 'Mirai' Released, KREBS ON SECURITY (Oct. 1, 2016), https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released.

42 *See* SentinelOne, *Mirai Botnet Descendants Will Lead to Even Bigger Internet Outages*, CSO (Dec. 22, 2016) https://www.csoonline.com/article/3153031/mirai-botnet-descendants-will-lead-to-even-bigger-internet-outages.html

43 *See, e.g.*, Grace Johansson, Satori Botnet Able to Launch Crippling Attacks at Any Time, SC MAGAZINE UK (Dec. 8, 2017), https://www.scmagazineuk.com/satori-botnet-able-launch-crippling-attacks-time/article/1473666; *See also* John Leyden, OMG, That's Downright Wicked: Botnet Authors Twist Corpse of Mirai into New Threats, THE REGISTER (June 1, 2018), https://www.theregister.co.uk/2018/06/01/mirai_respun_in_new_botnets.

44 Chris Bing, You can Now Buy a Mirai-Powered Botnet on the Dark Web, CYBERSECOOP (Oct. 27, 2016), https://www.cyberscoop.com/mirai-botnet-for-sale-ddos-dark-web.

45 Catalin Cimpanu, Liberian ISP Sues Rival for Hiring Hacker to Attack Its Network, ZDNET (Jan. 14, 2019), https://www.zdnet.com/article/liberian-isp-sues-rival-for-hiring-hacker-to-attack-its-network.

46 *Id.*

47 *Id.*

48 Brian Krebs, Powerful New DDoS Method Adds Extortion, KREBS ON SECURITY (Mar. 2, 2018), https://krebsonsecurity.com/tag/memcached-attack.

49 *Id.*

50 *Id.*

51 Cloudflare, Memcached DDoS Attack, https://www.cloudflare.com/learning/ddos/memcached-ddos-attack (last accessed Mar. 29, 2019).

52 Lily Newman, *Github Survived the Biggest DDOS Attack Ever Recorded*, WIRED (Mar. 1, 2018) https://www.wired.com/story/github-ddos-memcached.

53 Iain Thomson, *World's Biggest DDoS Attack Record Broken After Just Five Days*, THE REGISTER (Mar. 5, 2018), https://www.theregister.co.uk/2018/03/05/worlds_biggest_ddos_attack_record_broken_after_just_five_days.

54 Kacy Zurkus, *Largest DDoS Attack Sent Over 500 Million Packets per Second*, INFOSECURITY MAGAZINE (Jan. 30, 2019), https://www.infosecurity-magazine.com/news/largest-ddos-attack-sent-over-500

55 *Id.*

56 See Stephanie Weagle, *Short, Low-volume DDoS Attacks Pose Greatest Security and Availability Threat to Businesses*, ITPROPORTAL (July 7, 2017), https://www.itproportal.com/features/short-low-volume-ddos-attacks-pose-greatest-security-and-availability-threat-to-businesses.

57 *See, e.g.*, Dan Goodin, *Russian-controlled Telecom Hijacks Financial Services' Internet Traffic*, ARS TECHNICA (Apr. 27, 2017), https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic.

58 *See, e.g.*, Ms. Smith, *Possible BGP Hijacking Takes Google Down*, *CSO* (Nov. 13, 2018), https://www.csoonline.com/article/3320996/possible-bgp-hijacking-takes-google-down.html (explaining why a BGP incident could be perceived as a "war-game experiment").

59 Nate Anderson, H*ow China Swallowed 15% of 'Net Traffic for 18 Minutes*, ARS TECHNICA (Nov. 17, 2010), https://arstechnica.com/information-technology/2010/11/how-china-swallowed-15-of-net-traffic-for-18-minutes.

60 *Id.*

61 *Id.*

62 *Id.*

63 *See, e.g.*, Dan Goodin, *Russian-controlled Telecom Hijacks Financial Services' Internet Traffic*, ARS TECHNICA (Apr. 27, 2017), https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic.

64 *Id.*

65 Dan Goodin, *"Suspicious" event routes traffic for big-name sites through Russia*, ARS TECHNICA (Dec. 13, 2017), https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic.

66 Ms. Smith, *Possible BGP Hijacking Takes Google Down*, *CSO* (Nov. 13, 2018), https://www.csoonline.com/article/3320996/possible-bgp-hijacking-takes-google-down.html.

67 Jane Lanhee Lee and Paresh Dave, *Nigerian Firm Takes Blame for Routing Google Traffic Through China*, REUTERS (Nov. 13, 2018), https://www.reuters.com/article/us-alphabet-disruption/nigerian-firm-takes-blame-for-routing-google-traffic-through-china-idUSKCN1NI2D9.

68 Emma Woollacott, *If China Isn't Hijacking Internet Traffic, There's No Reason Why Not*, FORBES (Nov. 13, 2018), https://www.forbes.com/sites/emmawoollacott/2018/11/13/if-china-isnt-hijacking-internet-traffic-theres-no-reason-why-not/#24152e8e5ed5.

69 Veracode, *Cache Poisoning*, https://www.veracode.com/security/cache-poisoning (last accessed Apr. 2, 2019).

70 *See, e.g.*, Robert McMillan, *China's Great Firewall Spreads Overseas*, COMPUTERWORLD (Mar. 25, 2010), https://www.computerworld.com/article/2516831/security0/china-s-great-firewall-spreads-overseas.html.

71 Muks Hirani et al., *Global DNS Hijacking Campaign: DNS Record Manipulation at Scale*, FIREEYE (Jan. 9, 2019), https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html.

72 *Id.*

73 *Id.*

74 *Id.*

75 *Id.*

76 *Id.*

77 *Id.*

78 Muks Hirani et al., *Global DNS Hijacking Campaign: DNS Record Manipulation at Scale*, FIREEYE (Jan. 9, 2019), https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html.

79 Lily Newman, *A Worldwide Hacking Spree Uses DNS Trickery to Nab Data*, WIRED (Jan. 11, 2019), https://www.wired.com/story/iran-dns-hijacking.

80 *Id.*

81 *Id.*

82 See Maria Korolov, *Open Source Software Security Challenges Persist*, CSO (Oct. 4, 2018), https://www.csoonline.com/article/3157377/open-source-software-security-challenges-persist.html (citing a study where the average application had 147 different open source components).

83 *Id.*

84 Robert Hackett, T*housands of Companies Are Still Downloading the Vulnerability That Wrecked Equifax*, FORTUNE (May 7, 2018), http://fortune.com/2018/05/07/security-equifax-vulnerability-download.

85 *Id.*

86 *Id.*

87 *Id.*

88 *Id.*

89 *Id.*

90 Veracode, *Open Source Vulnerabilities*, https://www.veracode.com/security/open-source-vulnerabilities (last accessed Apr. 2, 2019).

91 *See, e.g.*, NTIA, Software Component Transparency, https://www.ntia.doc.gov/SoftwareTransparency.

92 Kelly Sheridan, *Microsoft Office: The Go-To Platform for Zero-Day Exploits*, DARK READING (June 21, 2019), https://www.darkreading.com/cloud/microsoft-office-the-go-to-platform-for-zero-day-exploits/d/d-id/1332114.

93 *Id.*

94 Catalin Cimpanu, *Microsoft Releases Security Update for New IE Zero-Day*, ZDNET (Dec. 19, 2018), https://www.zdnet.com/article/microsoft-releases-security-update-for-new-ie-zero-day.

95 Charlie Osborne, Lazarus Group Used ActiveX Zero-Day Vulnerability to Attack South Korean Security Think Tank, ZDNET (June 13, 2018), https://www.zdnet.com/article/north-korea-linked-lazarus-group-attacked-south-korean-think-tank-through-activex-zero-day.

96 *Id.*

97 James Doubek, *Government Outlines When It Will Disclose Or Exploit Software Vulnerabilities*, NPR (Nov. 17, 2017), https://www.npr.org/sections/alltechconsidered/2017/11/17/564755961/government-outlines-when-it-will-disclose-or-exploit-software-vulnerabilities.

98 *Id.*

99 *Id.*

100 Josh Fruhlinger, *Spectre and Meltdown Explained: What They Are, How They Work, What's at Risk*, CSO (Jan. 15, 2018) https://www.csoonline.com/article/3247868/vulnerabilities/spectre-and-meltdown-explained-what-they-are-how-they-work-whats-at-risk.html.

101 THE CENTER FOR CYBERSECURITY POLICY AND LAW, IMPROVING HARDWARE COMPONENT VULNERABILITY DISCLOSURE (2019) 3, https://centerforcybersecuritypolicy.org/improving-hardware-component-vulnerability-disclosure.

102 *Id.* at 5—6. *See also* Digital Europe, Joint industry letter on Cybersecurity Vulnerabilities Administrative Regulation Response to MIIT published draft for comments (July 19, 2019), https://www.digitaleurope.org/resources/joint-industry-letter-on-cybersecurity-vulnerabilities-administrative-regulation-response-to-miit-published-draft-for-comments/.

103 *Id.* at 3.

104 *Id.* at 5—6.

105 *See, e.g.*, CISA, *CISA's ICT Supply Chain Risk Management Task Force Launches Work Streams*, DEP'T OF HOMELAND SEC. (Feb. 26, 2019), https://www.dhs.gov/cisa/news/2019/02/26/cisa-s-ict-supply-chain-risk-management-task-force-launches-work-streams.

106 Tom Simonite, *NSA's Own Hardware Backdoors May Still Be a "Problem from Hell"*, MIT TECH. REVIEW (Oct. 8, 2013), https://www.technologyreview.com/s/519661/nsas-own-hardware-backdoors-may-still-be-a-problem-from-hell.

107 See Dan Goodin, *Major US Telecom was Infiltrated by Backdoored Supermicro Hardware, Bloomberg Says*, ARS TECHNICA (Oct. 9, 2018), https://arstechnica.com/gadgets/2018/10/new-bloomberg-report-says-backdoored-supermicro-hardware-infiltrated-major-us-telecom.

108 Charlie Osborne, *Apple, Amazon Deny Claims Chinese Spies Implanted Backdoor Chips in Company Hardware: Report*, ZD NET (Oct. 4, 2018), https://www.zdnet.com/article/how-one-tiny-chinese-chip-was-used-to-infiltrate-apple-amazon-us-contractors-report.

109 ICS-CERT, Dep't of Homeland Sec., *Destructive Malware 1* (2017), https://ics-cert.us-cert.gov/sites/default/files/documents/Destructive_Malware_White_Paper_S508C.pdf.

110 *Id.*

111 *See* Tara Seals, *Secrets of the Wiper: Inside the World's Most Destructive Malware*, THREATPOST (May 10, 2018), https://threatpost.com/secrets-of-the-wiper-inside-the-worlds-most-destructive-malware/131836 (discussing how destructive malware can target "files (data), the boot section of the operating system of machines, and backups of system and data").

112 Telefónica, *How Wiper Malware Affects Middle East and South America* 3 (2017), https://www.elevenpaths.com/wp-content/uploads/2018/07/informe-impacto-del-malware-de-tipo-wiper-en.pdf.

113 Symantec Security Response, *Shamoon: Back from the Dead and Destructive as Ever*, SYMANTEC (Nov. 30, 2016), https://www.symantec.com/connect/blogs/shamoon-back-dead-and-destructive-ever; Alexandre Mundo et al., *Shamoon Returns to Wipe Systems in Middle East, Europe*, MCAFEE (Dec. 14, 2018), https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/shamoon-returns-to-wipe-systems-in-middle-east-europe.

114 Tara Seals, *Shamoon Reappears, Poised for a New Wiper Attack*, THREATPOST (Dec. 13, 2018), https://threatpost.com/shamoon-new-wiper-attack/139881.

115 Jose Pagliery, The Inside Story of the Biggest Hack in History, CNN (Aug. 5, 2015) https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html.

116 *Id.*

117 Symantec Security Response, *Shamoon: Back from the Dead and Destructive as Ever*, SYMANTEC (Nov. 30, 2016), https://www.symantec.com/connect/blogs/shamoon-back-dead-and-destructive-ever.

118 Security Response Attack Investigation Team, *Shamoon: Destructive Threat Re-Emerges with New Sting in its Tail*, SYMANETC (Dec. 14, 2018), https://www.symantec.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail.

119 *Id.*

120 Adam Vincent, *BlackEnergy Malware: How Hackers May Tackle our Infrastructure*, INFOSECURITY (Feb. 7, 2018), https://www.infosecurity-magazine.com/opinions/blackenergy-malware-infrastructure.

121 *Id.*

122 ESET, *Grey Energy: A Successor to Black Energy* (Oct. 17, 2018), https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf; *See also* Sonal Patel, *BlackEnergy, Grid-Disrupting Malware, Has a Successor, Researchers Warn*, POWER (Oct. 18, 2018), https://www.powermag.com/blackenergy-grid-disrupting-malware-has-a-successor-researchers-warn/?pagenum=1.

123 Symantec Security Response, *Destructive Malware: An Ever-Evolving Threat*, MEDIUM (Mar. 23, 2017), https://medium.com/threat-intel/destructive-malware-evolution-392d3f8ef9d2.

124 Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

125 *Id.*

126 *Id.*

127 Danny Palmer, *This Destructive Wiper Ransomware was Used to Hide a Stealthy Hacking Campaign*, ZDNET (Nov. 1, 2017), https://www.zdnet.com/article/this-destructive-wiper-ransomware-was-used-to-hide-a-stealthy-hacking-campaign.

128 Assaf Dahan, *Night of the Devil: Ransomware or Wiper*, CYBEREASON (Oct. 31, 2017), https://www.cybereason.com/blog/night-of-the-devil-ransomware-or-wiper-a-look-into-targeted-attacks-in-japan (noting that "targeted attacks involving ransomware/wipers have been on the rise across the world in recent years").

129 *See, e.g.*, Lindsey O'Donnel, *Ransomware Behind Norsk Hydro Attack Takes On Wiper-Like Capabilities*, THREATPOST (Mar. 27, 2019), https://threatpost.com/lockergoga-ransomware-norsk-hydro-wiper/143181 (noting that at time of the article's publication "there has been no attribution to the attack, adding into the mystery when it comes to the malware developers' underlying goals.").

130 Nicole Perlroth, *Cyberattack Caused Olympic Opening Ceremony Disruption*, N.Y. TIMES (Feb. 12, 2018), https://www.nytimes.com/2018/02/12/technology/winter-olympic-games-hack.html.

131 Warren Mercer and Paul Rascagneres, *Olympic Destroyer Takes Aim At Winter Olympics*, CISCO (Feb. 12, 2018), https://blog.talosintelligence.com/2018/02/olympic-destroyer.html.

132 Andy Greenberg, S*tealthy, Destructive Malware Destroys Half a Million Routers*, WIRED (May 23, 2018), https://www.wired.com/story/vpnfilter-router-malware-outbreak.

133 *See* CISA, Dept' of Homeland Sec., *VPNFilter Destructive Malware* (May 23, 2018), https://www.us-cert.gov/ncas/current-activity/2018/05/23/VPNFilter-Destructive-Malware (classifying VPNFilter as destructive malware).

134 Andy Greenberg, *Stealthy, Destructive Malware Destroys Half a Million Routers*, WIRED (May 23, 2018), https://www.wired.com/story/vpnfilter-router-malware-outbreak.

135 *Id.*

136 Alan Blinder and Nicole Perlroth, *A Cyberattack Hobbles Atlanta, and Security Experts Shudder* (Mar. 27, 2018), N.Y. TIMES https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html.

137 Emerging Technology from the arXiv, *True Scale of Bitcoin Ransomware Extortion Revealed*, MIT TECH. REVIEW (Apr. 19, 2018), https://www.technologyreview.com/s/610803/true-scale-of-bitcoin-ransomware-extortion-revealed.

138 Alan Blinder and Nicole Perlroth, *A Cyberattack Hobbles Atlanta, and Security Experts Shudder* (Mar. 27, 2018), N.Y. TIMES https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html.

139 *Id.*

140 *Id.*

141 *Id.*

142 Catalin Cimpanu, *How US Authorities Tracked Down the North Korean Hacker Behind WannaCry*, ZDNET (Sept. 6, 2018), https://www.zdnet.com/article/how-us-authorities-tracked-down-the-north-korean-hacker-behind-wannacry.

143 Alexander Smith et al., *Why 'WannaCry' Malware Caused Chaos for National Health Service in U.K.* (May 17, 2017), https://www.nbcnews.com/news/world/why-wannacry-malware-caused-chaos-national-health-service-u-k-n760126.

144 Stu Sjouwerman, *The Rise of Ransomware-as-a-Service*, CSO (Dec. 12, 2016), https://www.csoonline.com/article/3147815/the-rise-of-ransomware-as-a-service.html.

145 SentinelOne, Ransomware as a Service: Hacking Made Easy, CSO (Jan. 31, 2017), https://www.csoonline.com/article/3163526/ransomware-as-a-service-hacking-made-easy.html.

146 *See* David Bisson, *The Top 10 Ransomware Strains of 2016*, TRIPWIRE (Dec. 18, 2016), https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/top-10-ransomware-strains-2016.

147 Andy Greenberg, *The White House Blames Russia for NotPetya, the "Most Costly Cyber Attack in History"*, WIRED (Feb. 15, 2018), https://www.wired.com/story/white-house-russia-notpetya-attribution.

148 *Id.*

149 *Id.*

150 *Id.*

151 ENISA, *Supply Chain Attacks* (Aug. 29, 2017), https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks.

152 *See, e.g.*, Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

153 See Bradley Barth, *Fresh-faced Anatova Ransomware Created by 'Skilled Developers,' Researchers Warn*, SC MAGAZINE UK (Jan. 23, 2019), https://www.scmagazineuk.com/satori-botnet-able-launch-crippling-attacks-time/article/1473666

154 *Id.*

155 *Id.*

156 *Id.*

157 Nicole Perlroth and Clifford Krauss, A *Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try*, N.Y. TIMES (Mar. 15, 2018), https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html.

158 *Id.*

159 *Id.*

160 *Id.*

161 Sean Lyngaas, *FireEye Links Russia-owned Lab to Group Behind Trisis*, CYBERSCOOP (Oct. 23, 2018), https://www.cyberscoop.com/trisis-russia-fireeye.

162 *Id.*

163 Chris Bing, *Trisis Masterminds have Expanded Operations to Target U.S. Industrial Firms*, CYBERSCOOP (May 24, 2018), https://www.cyberscoop.com/xenotime-ics-cyber-attacks-trisis-dragos.

164 *Id.*

165 *See, e.g.*, U.S. CERT, Dep't of Homeland Sec., *Advanced Persistent Threat Activity Exploiting Managed Service Providers* (Oct. 3, 2018) https://www.us-cert.gov/ncas/alerts/TA18-276B.

166 Chris Bing, *Trisis Masterminds have Expanded Operations to Target U.S. Industrial Firms*, CYBERSCOOP (May 24, 2018), https://www.cyberscoop.com/xenotime-ics-cyber-attacks-trisis-dragos.

167 Stilgherrian, At Least Nine Global MSPs Hit in APT10 attacks: ACSC, ZDNET (Dec. 21, 2018), https://www.zdnet.com/article/at-least-nine-global-msps-hit-in-apt10-attacks-acsc.

168 *Id.*; *See also* Jai Vijayan, China-Based Threat Actor APT10 Ramps Up Cyber Espionage Activity, DARK READING (Apr. 6, 2017), https://www.darkreading.com/attacks-breaches/china-based-threat-actor-apt10-ramps-up-cyber-espionage-activity/d/d-id/1328584.

169 FireEye, APT10, https://www.fireeye.com/current-threats/apt-groups.html#apt10 (last accessed Mar. 29, 2019); *See also* William Tsing, *The Advanced Persistent Threat files: APT10*, MALWAREBYTES (Jan. 16, 2019), https://blog.malwarebytes.com/cybercrime/2019/01/advanced-persistent-threat-files-apt10.

170 Stilgherrian, At Least Nine Global MSPs Hit in APT10 attacks: ACSC, ZDNET (Dec. 21, 2018), https://www.zdnet.com/article/at-least-nine-global-msps-hit-in-apt10-attacks-acsc.

171 Jai Vijayan, *APT10 Indictments Show Expansion of MSP Targeting, Cloud Hopper Campaign*, DARK READING (Dec. 21, 2018), https://www.darkreading.com/threat-intelligence/apt10-indictments-show-expansion-of-msp-targeting-cloud-hopper-campaign/d/d-id/1333539; *See also* PwC UK and Bae Systems, OPERATION CLOUD HOPPER (Apr. 2017), https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf.

172 *Id.*

173 Dark Reading Staff, *Chinese APT10 Hacking Group Suspected of Global Campaign Targeting MSPs*, DARK READING (Apr. 5, 2017), https://www.darkreading.com/attacks-breaches/chinese-apt10-hacking-group-suspected-of-global-campaign-targeting-msps/d/d-id/1328563.

174 Davis Bond, *Hackers Target Cloud Services*, FINANCIAL TIMES (July 12, 2018), https://www.ft.com/content/4f990a78-537a-11e8-84f4-43d65af59d43 (discussing PwC's analysis of Operation Cloud Hopper in the context of supply chain risk); Jai Vijayan, *APT10 Indictments Show Expansion of MSP Targeting, Cloud Hopper Campaign*, DARK READING (Dec. 21, 2018), https://www.darkreading.com/threat-intelligence/apt10-indictments-show-expansion-of-msp-targeting-cloud-hopper-campaign/d/d-id/1333539 (quoting FireEye's senior manager of cyber espionage as stating that APT10's "move towards compromising managed service providers (MSPs) showcases the danger of supply chain compromises and reflects their continuously evolving tactics").

175 Maria Deutscher, *New Cloudborne Vulnerability Exposes Cloud Servers to Potential Hacking*, SILICONANGLE (Feb. 26, 2019), https://siliconangle.com/2019/02/26/new-cloudborne-vulnerability-potentially-exposes-cloud-servers-hacking.

176 *Id.*

177 *Id.*

178 Ponemon Institute, 2017 COST OF DATA BREACH STUDY (June 2017), https://www.ibm.com/downloads/cas/ZYKLN2E3.

179 *See* Susan Landau, *Understanding Data Breaches as National Security Threats*, LAWFARE BLOG (Feb. 26, 2018), https://www.lawfareblog.com/understanding-data-breaches-national-security-threats.

180 Tim Worstall, *Lloyd's - Extreme Cyberattack Could Cost $120 Billion, As Much As 0.2% Of Global GDP*, FORBES (July 17, 2017), https://www.forbes.com/sites/timworstall/2017/07/17/lloyds-extreme-cyberattack-could-cost-120-billion-as-much-as-0-2-of-global-gdp/#20d26ed46cc3.

181 *Id.*

182 *Compare* Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world (discussing the $10 billion damages caused by NotPetya) *with* Tim Worstall, *Lloyd's - Extreme Cyberattack Could Cost $120 Billion, As Much As 0.2% Of Global GDP*, FORBES (July 17, 2017), https://www.forbes.com/sites/timworstall/2017/07/17/lloyds-extreme-cyberattack-could-cost-120-billion-as-much-as-0-2-of-global-gdp/#20d26ed46cc3.

183 CNN, *Hurricane Sandy Fast Facts*, https://www.cnn.com/2013/07/13/world/americas/hurricane-sandy-fast-facts/index.html (last accessed Apr. 2, 2019).

184 Danny Palmer, *Cloud computing: Why a Major Cyber-Attack Could Be as Costly as a Hurricane*, ZDNET (Jan. 17, 2018), https://www.zdnet.com/article/cloud-computing-why-a-major-cyber-attack-could-be-as-costly-as-a-hurricane.

185 Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

securingdigitaleconomy.org