Chapter 1

NATIONAL CYBER RESILIENCE AND ROLES FOR PUBLIC AND PRIVATE SECTOR STAKEHOLDERS

Neal Ziring

Abstract Modern nations are dependent on cyberspace, specifically, on information technology, data communications, smart mobile devices and other globally-connected and computing-enabled services. The dependence includes government operations, national defense, critical infrastructure and economic prosperity. However, cyberspace is subject to accidental disruptions and malicious attacks from a wide variety of sources. Therefore, to ensure resilient functioning, every nation must possess a resilient cyberspace. This chapter describes a model for large-scale (regional to national) resilience of cyberspace, describes mechanisms for applying the model to improve overall national resilience and identifies key stakeholders for implementing the mechanisms in the United States.

Keywords: Cyber security, public sector, private sector, cyber resilience

1. Introduction

The United States and other modern nations depend on a broad set of critical infrastructures to support their populations. The infrastructures depend on each other in multiple ways, but in the most general sense, they form a web of interdependencies such that a sustained disruption of one infrastructure can degrade or halt operations in other infrastructures [22, 74]. For example, the financial system depends on the power grid – banks cannot operate for long without electricity. Interdependencies in multiple critical infrastructures is a broad subject area. This work assumes that national functions, including other critical infrastructures, depend on the availability and reliability of the cyber infrastructure. Therefore, to minimize disruptions of national functions,

Published by Springer Nature Switzerland AG 2022
J. Staggs and S. Shenoi (Eds.): Critical Infrastructure Protection XVI, IFIP AICT 666, pp. 3–46, 2022.
https://doi.org/10.1007/978-3-031-20137-0_1

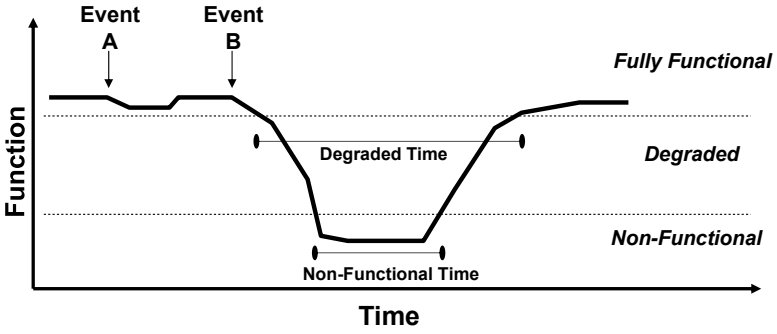

Figure 1. Impact of a disruptive event.

and bolster national security, economic prosperity and societal wellbeing, every nation should ensure that its cyber infrastructure is resilient – resistant to disruptions and attacks and quick to recover.

Resilient cyber infrastructure must be created in a deliberate manner – resilience requires intentional design and focused operation. This chapter defines the properties of a resilient cyber infrastructure, presents a model for achieving resilience at large scales and applies the model at a national scale using the United States as exemplar. Naturally, the operation of any cyber infrastructure depends on other critical infrastructures such as power and transportation. However, the composition and reliability of these infrastructures at a large scale, albeit critical, are outside the scope of this work.

Before considering the properties of resilient cyber infrastructure, it is necessary to select a definition of resilience and a bounded scope for the cyber infrastructure. Resilience is defined in the U.S. national security strategy [33] and other national security documents as "the ability to withstand and recover rapidly from deliberate attacks, accidents, natural disasters, as well as unconventional stresses, shocks and threats." This definition, like others, incorporates two essential elements, the ability to resist degradation and disruption (withstand) and the ability to recover from disruptions that it cannot resist.

One way of measuring the resilience of a service is to characterize the events that impact service functionality and the duration and severity of the impacts. Figure 1 presents the impact of a disruptive event based on the general model presented by Cybenko [21]. The notional service in the figure has a level of functionality that its users expect. Anything above this level is considered to be fully functional. Levels of functionality below the level, but still above some minimum, are considered to be

degraded operations. Service below the minimum level is considered to be non-functional.

The service in Figure 1 withstands Event A; there is some impact, but the service remains fully functional. However, the service experiences a serious impact from Event B; it is non-functional for a certain duration and degraded for a longer duration. In practical terms, the resilience of a service is greater when it can withstand more salient events and when the degraded and non-functional durations are shorter.

Cyber infrastructure is a complicated term with no standard definition. The term came into common use after a 2003 report by a U.S. National Science Foundation advisory panel on cyber infrastructure [8]; interestingly, the panel report focused on infrastructure for supporting research.

The U.S. communications infrastructure sector is formally defined by the U.S. Department of Homeland Security (DHS) [22]. However, this sector partially overlaps with cyber infrastructure because the communications sector definition omits the computation, storage, discovery and automated service facets of cyberspace.

Several articles described in the related work section below offer definitions of cyber infrastructure. They are all reasonable, but they lack consistency and detail. They were used as inputs to arrive at the definition used in this work.

In this work, cyber infrastructure is defined as comprising four high-level categories according to the model described in [82]:

- **Physical Support Elements:** These elements include facilities, buildings, cables, antennas, towers, satellites and other physical artifacts that host the cyber infrastructure.

- **Communications Elements:** These elements support the transfer of data between users and infrastructure services, among users and between other elements of the infrastructure. The elements include control systems and overlays that facilitate or manage the communications. Communications elements can be subdivided further in many ways, but in this work, the salient division is between the communications links and the control systems that monitor and manage the links.

- **Computation and Storage Elements:** These elements correspond to the services that support cyberspace users by providing search and retrieval, information management and state update functionality. The category includes three sub-categories:

  - Registration, provisioning and discovery services that support the operation of higher-level services.
  - Security services, including foundational services that support identification, authentication, access control and integrity.
  - Platform services and shared infrastructure elements that provide computational and storage resources to users.

- **Business and Governance Elements:** These elements correspond to user-level processes that oversee and enable the infrastructure. The elements include economic processes such as billing and financing, regulatory regimes and stakeholder governance.

Detailed lists of technologies and services that comprise the four categories listed above are presented later in this chapter. The resilience analysis described in this work focuses primarily on the communications element and the computation and storage element categories. However, the implementation of resilience improvements would affect all the categories and would require the addition of resilience as a goal in the business and governance element category.

2. Related Work

This section discusses the literature related to cyber infrastructure threats and cyber infrastructure resilience.

2.1 Cyber Infrastructure Threats

The rich literature on cyber threats and associated security measures dates back to early threats against communications and information systems. Several historical surveys have been published that offer differing views of how threats have been addressed from an information-centric perspective [25] to an emphasis on cryptology [50].

Security threats to computer systems gained attention in the 1960s with the advent of multi-user and time-sharing systems. The early computers were not, typically, connected to each other, and security controls were focused on local threats such as unauthorized data access (confidentiality threat) and interference with shared system functionality (availability threat). A fascinating early example of threats to virtual machine infrastructures covers denial of service and theft of data [58]. Most of the early work was not systematic, focusing on specific threats to, and security features of, specific systems (e.g., Adept-50 system [92]) and on the theoretical foundations of system design (e.g., Saltzer and Schroeder's seminal work [77]). The first systematic treatment was the U.S. Department of Defense's technical evaluation criteria for secure computer sys-

tems (TCSEC) proposed in 1979 [64] and codified in 1985 [86]. Despite the emphasis on confidentiality implicit in TCSEC, it defined a rigorous approach to enumerating threat mitigation controls and evaluating their implementation.

The growth of computer networks in the 1980s and early 1990s drew attention to threats against computer networks and their underlying communications. The earliest treatment of threats to large-scale networks such as the Internet was published in 1983 [91].

Modern treatments of cyber infrastructure threats focus on two broad areas, threats to the communications infrastructure from all sources and cyber threats to critical infrastructures in general. A good example of the former is a 2010 survey by Sterbenz et al. [81] on the resilience of communications networks. Threats to critical infrastructure and mitigating them gained national attention in the United States in the mid-1990s, culminating in the creation of the President's Commission on Critical Infrastructure Protection [16]. Emphasis on cyber threats emerged in the early 2000s after Internet worms demonstrated that cyber attacks could cause serious harm to businesses and government [62].

Around the same time, in the late 1990s and early 2000s, the national security community began to focus on risks posed by state and non-state actors that leverage cyber means to advance national aims or conduct large-scale attacks [27, 54, 72]. As evidence of cyber warfare programs emerged over the decade, practical concerns about threats and effective responses gained attention [40].

As cyber infrastructure diversified over the first two decades of the 21st century, considerable research focused on threats and resilience related to cyber infrastructure in general [31] as well as specific infrastructure components. Examples of the latter include the routing infrastructure [14], Domain Name System [7] and transoceanic cables [69]. As companies and governments adopted cloud computing services, researchers noted the broad spectrum of threats to the cloud, including their reliance on other cyber infrastructures [76]. With the emergence of the Internet of Things as a concept in the early 2000s and the proliferation of connected objects starting around 2010, the potential for cyber attacks to affect the physical world has greatly increased. Threat and security research on the Internet of Things has been very active since 2010; recent publications with broad coverage include [1, 12].

2.2 Cyber Infrastructure Resilience

The topic of resilience has been researched for decades and applied to communications and computing systems for nearly as long as the tech-

nologies have existed. This review covers work that directly contributes to the analysis and improvement of cyber resilience at a large scale.

Several studies have focused on failures of the Internet and its infrastructure dating back to the first Internet worm [80]. More recent assessments have examined the Internet and its core infrastructures with the intent of characterizing failure modes to inform improvements [30, 93]. The long-term evolution of denial-of-service attacks, from the late 1990s to the present day, has been examined in many ways; a good survey is provided by Mansfield-Devine [59].

General studies of infrastructure resilience have been undertaken by researchers around the world, many of them focus on resilience to natural disasters (see, e.g., [11]). General [9] and cyber-specific [56] models have been proposed for measuring resilience, as well as models for engineering resilient cyber systems [10].

As the reliance of the U.S. military on networks and cyber services increased, national defense analysts became concerned about cyber threats to military operations. This concern led to an in-depth study by the U.S. Defense Science Board that recommended measures for making military operations resilient to advanced cyber threats [26].

The cyber infrastructure has been recognized as a salient aspect of national security and its defense and resilience are vital to the overall national security posture. An exceptional treatment is the coverage of the role of cyberspace in the national security posture of the United Kingdom [19]. Military requirements for cyber capabilities as part of national defense appear consistently in U.S. defense strategy documents since 2005.

3. Cyber Infrastructure and Threats

Cyber infrastructure is a complex and dynamic fabric comprising multiple technologies and services. This section presents a simple layered model for cyber infrastructure and describes the threats to the large-scale operation of cyber infrastructure organized according to the layered model.

3.1 Cyber Infrastructure Model

A wide variety of technologies, standards, practices and systems underpin the modern cyber infrastructure. The infrastructure components depend on each other in complex ways, but can be envisioned as a set of layers where each layer depends primarily on the layers beneath it.

Figure 2 shows the basic cyber infrastructure layers. Each layer comprises multiple services with complex dependencies. For reasons of space,

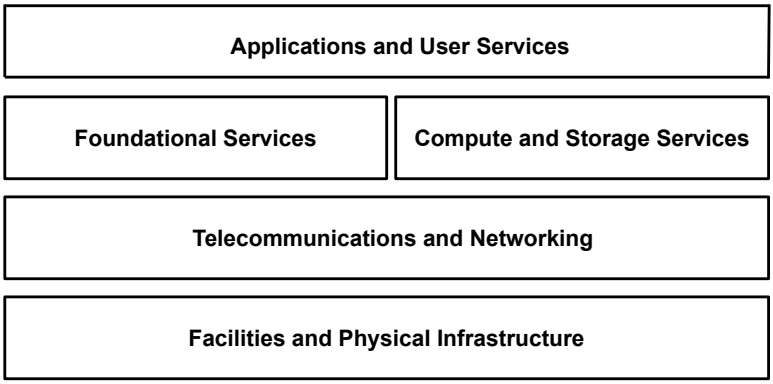

Figure 2. Basic cyber infrastructure layers.

it is not possible to describe all the services in detail; however, references are provided to technical details about the services. Additionally, a large body of mature engineering and operational expertise exists for the bottom facilities and physical infrastructure layer and the top applications and user services layer. Therefore, this chapter focuses on the middle layers, the foundational services, compute and storage services, and telecommunications and networking layers.

The foundational services layer provides the functionality that supports the applications and user services layer. This includes services for discovery, information distribution and security. Table 1 describes the five main elements of the foundational services layer. Interested readers are referred to [5, 6, 29] for details about the foundational services layer.

The compute and storage services layer provides services that host operational systems and services employed by enterprises, which are vital to customers, partners and citizens. In the early days of computing, most enterprises simply purchased computing hardware and operated the equipment in their own facilities. However, public and private enterprises often rely on external service providers for storage, compute, data dissemination, office automation and numerous other services. The dependence on external providers is growing steadily; in 2018, 73% of businesses worldwide hosted some of their applications externally [47]. Table 2 describes the four main elements of the compute and storage services layer.

The telecommunications and networking layer orchestrates the movement of data traffic that supports the upper layers of the cyber infrastructure. Also, it provides connectivity and user-to-user communications services to subscribers, which include enterprises and individuals. Ta-

Table 1. Foundational services layer elements.

Element	Description
Domain Name System	The Domain Name System (DNS) provides translations between hierarchical names (e.g., `www.gwu.edu`) and network addresses (e.g., `104.17.56.239`). Also, it provides look-up for services (e.g., email) to service endpoints [17, 57].
Email	Email services, employing multiple protocols (ESMTP, POP, IMAP) and data formats (MIME, S/MIME), are used for reliable store-and-forward transfer of short messages and files [17, 20].
Web	The World Wide Web (WWW) infrastructure provides services over unsecured (HTTP) and secured (HTTPS) connections that support human and machine interactions [17].
Messaging	Several real-time messaging services are offered in cyberspace for communications between users and as foundational services for distributed applications. This service category is not effectively standardized, but it underlies a range of mobile, web and business applications (distinct from the Short Message Service provided by the telecommunications layer) [32, 49].
Public Key Infrastructure	A public key infrastructure (PKI) provides services for issuing trust artifacts (keys and certificates) and validating them [44].

Table 2. Compute and storage services layer elements.

Element	Description
Utility Compute	Computational services support business, mission and academic applications. The services are offered via diverse delivery models and often support reliability and disaster recovery.
Storage, Backup and Retrieval	Storage services are offered via various models and typically provide long-term storage and retrieval with availability and latency guarantees. The services support reliability and disaster recovery.
Content Delivery	Delivery services support large-scale data dissemination for various purposes. Most software downloads for establishing and maintaining enterprise applications employ these services.
Business Services	Compute and storage providers offer a variety of aggregated and hosted business services that support resource management, logistics, financial transactions and human capital management.

Table 3. Telecommunications and networking layer elements.

Element	Description
Subscriber Connectivity	Telecommunications carriers provide connection services for data and voice at regional, national and international levels. These include direct (cable and fiber) connections and wireless (cellular and other radio frequency) connections [35].
Voice Service	Telecommunications carriers cooperate to offer direct voice service between subscribers as well as various supporting services such as multi-party conferencing and voicemail.
Short Message Service	Telecommunications carriers cooperate to convey text messages and multimedia messages between mobile subscribers, and to transfer to various other services (e.g., email) [83].
Signaling	This global common channel signal control service supports voice and smart message services. Formerly based almost exclusively on the Signaling System 7 (SS7) standard [53], it is migrating to a mix of SS7 and newer standards [73].
Internet Protocol Routing	This global service for conveying Internet Protocol (IP) packets between cooperating telecommunications carriers is designed to be adaptive to changing demand, outages and other factors [45].
Link Switching	Telecommunications carriers depend on various link technologies and protocols to support wide-area network (WAN) connectivity such as optical links [78], multiprotocol label switching [90] and newer software-defined WAN approaches [60].
Time	Networks and services depend on accurate, synchronized time. Two primary synchronization protocols used on the Internet and by telecommunications carriers are the Network Time Protocol (NTP) and Precision Time Protocol (PTP) [51].

ble 3 describes the seven main elements of the telecommunications and networking layer.

The Internet Protocol (IP) routing element is especially important to the resilient operation of the contemporary Internet and other cyberspace services. In the current architecture, major carriers, governments, cloud providers and other large enterprises operate their own IP networks, each of which is an autonomous system. The autonomous systems connect to each other via dedicated gateways, but more often via Internet Exchange Points (IXPs) that connect several carriers and enterprises. Internet exchange points help define the operational topology of cyberspace at the national and international levels [42]. However, the topology is far from uniform. Historically, a small number of highly-

connected autonomous system operators (large telecommunications carriers) have underpinned national and global connectedness [34].

Autonomous system operators run Border Gateway Protocol (BGP) installations as cooperative members of the global routing fabric [45]. Participating in global BGP operations enables each autonomous system owner to offer reachability to its users and/or customers as well as to permit transit traffic in accordance with internal link status and business rules. Operated properly, BGP automatically adapts to outages, link failures and other state changes. However, it was not designed to withstand injections of false state information [14].

At the national and global levels, cyberspace depends on the IP routing element. This element depends, in turn, on many individual communications paths that constitute the link switching element. The links may be physical links over fiber optic cable or satellites or they may be overlays controlled by switching protocols such as multiprotocol label switching (MPLS) [90].

3.2 Cyber Infrastructure Threats

Cyber infrastructures face many of the same types of threats as other infrastructures – natural disasters, intentional sabotage, misuse and more. However, unlike most other critical infrastructures, a cyber infrastructure is not tightly bound to geography, in the sense that disruptions in one region may impose impacts much more broadly. Of the cyber infrastructure layers in Figure 2, successively higher layers are increasingly independent of physical location and more dependent on the abstract topology implemented by the other elements that they utilize. The complexity of individual elements and their interrelationships magnifies or spreads the impacts of threats, especially threats against elements in the lower layer that support all the higher layers.

Infrastructure threats can be subdivided along several axes – intentional versus accidental, localized versus wide-area, disruptive versus destructive and more. Special taxonomies have been published for many domains such as Internet security [15] and energy control system operations [36].

The following three axes relevant to impact severity are employed in the treatment of national-level resilience:

- **Intentionality:** This axis covers disruptions caused intentionally by malicious actors and accidents caused unintentionally by non-malicious actors. An implication is that malicious actors may adapt to mitigation and recovery measures.

- **Duration:** This axis covers the durations of disruptive events. A cable cut may be of short duration. A malicious denial-of-service attack may be long lasting. The effects of a serious flood may be extended. A key consideration is whether the events are one-time or recurring.

- **Reversibility:** This axis covers disruptions that can be reversed to a prior state easily to disruptions whose effects are enduring or even permanent. For example, crashing a set of servers is reversible by simply restarting them, but reversing the effects of wiping the servers may not be possible.

Tables 4 through 6 list potential large-scale threats to the infrastructure elements listed in Tables 1 through 3. In particular, Table 4 lists general threats that may be malicious or accidental. Tables 5 and 6 list intentional threats that are typically malicious.

The lists of threats are representative, not comprehensive. The threats are realistic because they have been demonstrated or experienced at a significant scale. National cyber resilience should ensure the ability to absorb these types of threats without serious degradation, and in extreme cases, recover within a timeframe that avoids significant economic, social or national security impacts. Members of the U.S. Defense Science Board [26] have recognized the potential for grave national security and economic impacts from malicious cyber attacks, and advocate increased resilience as a necessary countermeasure.

4. National-Scale Resilience Model

Economic, social and national security benefits associated with cyberspace accrue from the top layer of Figure 2, the applications and services used by public and private sector enterprises, academia and the general public. When these services are interrupted, cascading impacts ensue, as in the case of natural disasters such as Hurricane Sandy [18].

Therefore, if resistance to disruption and quick recovery in the lower layers can sustain the functionality of the top layer, then the overall cyber infrastructure may be regarded as resilient. A simple metric to consider is the value I_T from [21], the time interval when performance is below minimally acceptable values. In this case, performance denotes the usable operation of services in the top layer, namely, business, government and personal use of cyberspace. For example, if a hospital cannot provide treatment due to inaccessibility of medical records, then a lower value of I_T indicates greater resilience and a value of zero indicates full resilience. Access to medical records is a complex function that is depen-

Table 4. General threats to cyber infrastructure layers.

Threat	Applicability and Effects
Power Outage	A widespread power outage typically disrupts network services, especially subscriber connectivity across the affected region. If a region has major hubs in the Internet routing topology, impacts spread far beyond the region. *Duration:* Hours to days. *Reversibility:* Reversible.
Cable Cuts	Physical damage to critical data cables can cause regional network disruptions. Multiple cuts could partition national networks. *Duration:* Hours to weeks. *Reversibility:* Reversible.
Routing Failure	Degradation of the global routing process can result in regional or national loss of reachability. Impacts are highly variable. *Duration:* Minutes to hours. *Reversibility:* Reversible.
Internet Exchange Point Loss	Unavailability of an Internet exchange point (IPX) due to physical facility loss. The degraded connectivity impacts multiple carriers with broad service disruptions. *Duration:* Days to months. *Reversibility:* Variable.
Data Loss	Unavailability of large amounts of stored data due to facility failure or malicious deletion. Impacts users and all services that depend on the data. *Duration:* Hours to weeks. *Reversibility:* Variable.
Domain Name System Domain Loss	Unavailability or loss of integrity of a top-level domain (e.g., `.gov` or `.uk`) with impacts to tenants and users. *Duration:* Seconds to hours. *Reversibility:* Reversible.
Supply Chain Compromise	Disruption, service degradation or destruction via the malicious introduction of vulnerabilities in a product or product line. Impacts include regional, national or global loss of connectivity, service or integrity. An example is the 2002 multi-vendor SNMP vulnerability [84]. *Duration:* Unknown. *Reversibility:* Low, reconstitution is required.

dent on the foundational, compute and storage, and telecommunications and networking services described in Section 3.

Several studies of critical infrastructure risk have noted that fragility and vulnerability to cascading failures is a consequence of infrastruc-

Table 5. Intentional threats to cyber infrastructure layers.

Threat	**Applicability and Effects**
Route Hijacking	Malicious misrouting or non-routing of a range of network addresses. Impacts reachability of services and connectivity. *Duration:* Seconds to hours. *Reversibility:* Reversible.
Congestion Denial of Service	Degradation of service or connectivity imposed by flooding networks or service providers. Impacts all users of affected networks, even users outside the directly-affected area. *Duration:* Seconds to hours. *Reversibility:* Reversible.
Domain Name System Poisoning	Injection of false, misleading or malicious mappings in domains. A large-scale attack can disrupt services, degrade trust in services or support other large-scale malicious activities. *Duration:* Minutes to days. *Reversibility:* Variable.
Domain Name System Denial of Service	Degradation or interruption of DNS services by congestion, route hijacking or other mechanisms. Impacts to tenants and users of the affected domains; usually all the domains hosted by the victim DNS service provider. *Duration:* Minutes to hours. *Reversibility:* Reversible.
Widespread Malware Execution	Operation of disruptive or destructive software on numerous devices in a region, nation or industry verticals. Impacts due to congestion [62] and data destruction [43]. *Duration:* Hours to weeks. *Reversibility:* Variable.
Compute and Storage Denial of Service	Interrupted access to compute and storage services by resource consumption, misauthorization or other non-destructive means. Loss of higher-level business, government and user services. *Duration:* Minutes to days. *Reversibility:* Reversible.
Message System Flooding	Degradation or disruption of enterprise functions and user interactions that depend on the underlying message system. Severe impacts on affected industry verticals. *Duration:* Seconds to hours. *Reversibility:* Reversible.
Public Key Infrastructure Denial of Trust	Loss of ability to trust high-level web, email and application services due to compromises of trust foundations. Disruptions of business functions and user interactions [3]. *Duration:* Days to weeks. *Reversibility:* Difficult, reconstitution is required.

Table 6. Intentional threats to cyber infrastructure layers (continued).

Threat	Applicability and Effects
Signaling Denial of Service	Interruption or loss of integrity of signaling services that underpin voice and SMS services. Impacts single carriers, multiple carriers or the national network. *Duration:* Seconds to hours. *Reversibility:* Reversible.
Time Desynchrony	Loss of time synchronization in portions of networks degrades services until synchrony is restored. Impacts are varied. *Duration:* Seconds to hours. *Reversibility:* Reversible.

ture complexity [55, 61]. The common feature of the infrastructures cited in these studies is that they grew more complex over time without considering the resistance to attacks or efficient recovery from degraded operations. Studies in the electric energy sector have shown that complex infrastructure need not be fragile if it is engineered and operated for resilience [4].

4.1 Cyber Infrastructure and Resilience

Cyber infrastructure has several features that can help support resilient design and operation:

- Cyber infrastructure is amenable to highly detailed, accurate and responsive instrumentation. Response to adverse conditions requires the detection of these conditions. Cyber infrastructure is well-suited to timely detection.
- Cyber infrastructure is not static. Communications, compute and application services are defined largely by software, which can be updated and improved at a far lower cost than replacing the components. For example, network operators can implement software-defined wide-area networks using existing switch hardware without the capital investment of purchasing new switches [60].
- Cyber infrastructure operation is not bound to physical geography. Several elements of cyber infrastructure can and do function in a geographically-distributed manner. While this aspect of cyber infrastructure allows the impacts of disruptions to extend well beyond an initially-affected facility or region, it also permits distributed resilience – disruption in one region or even one nation

Table 7. Resilience engineering goals/stages.

MITRE Framework [10] "Goal"	**Linkov et al./ NAS [56] "Stage"**	**High-Level Description**
Anticipate	Plan/Prepare	Establish a state of informed preparation for disruptions or attacks, lay foundations and maintain awareness.
Withstand	Absorb	Continue operations through a disruption or attack, limit or minimize impacts, repel attack or isolate its effects.
Recover	Recover	Restore capability and capacity, assess damage and requirements for complete reconstitution.
Evolve	Adapt	Adjust architecture, processes, operations and system configurations to minimize future impacts and facilitate recovery.

can be mitigated to varying degrees by service offerings elsewhere. This is not true of all cyber infrastructure elements. A critical exception is subscriber connectivity, which is typically tied to geography.

These features support flexible implementation of resilience measures, enabling a nation to amortize investments across multiple sectors, regions and infrastructure elements to achieve resilience goals.

4.2 Basic Resilience Model

Two widely-cited sources on resilience engineering are the MITRE cyber resiliency engineering framework [10] and the work of Linkov et al. [56], which define four very similar basic parts, the latter based on previous work by the National Academy of Sciences (NAS). Table 7 describes the resilience engineering goals and stages in the two sources. The remainder of this chapter uses the MITRE terminology, but ideas from both sources are used in the discussion.

It is possible to measure many aspects of resilience based on the four goals in the MITRE framework. The metrics can inform planning and preparation, response during disruptions, priorities for recovery and areas for attention during evolution.

The MITRE resiliency engineering framework [56] is designed for application at enterprise scales, up to very large enterprises such as the

U.S. Department of Defense. At a national scale, additional issues come into play:

- Planning and preparation for large-scale disruptions or attacks are necessarily incomplete. It is not possible to enumerate all possible failure modes of complex interdependent systems or the impacts of cascading failures on the economy or society [11].
- National-scale cyber infrastructure is built, maintained, operated and regulated by multiple stakeholders with different degrees of visibility and control. These stakeholders have different motivations, but typically have little to no incentive to collaborate to improve the overall resilience [19, 55].
- Cyber infrastructure at the national scale is visible to and observable by almost anyone, include threat actors. In enterprise contexts, concealing or obscuring the properties of cyber infrastructure is a generally-accepted practice, but at the national scale, secrecy cannot be effective. For example, an enterprise can hide its internal network architecture, but the top-level topology of the Internet is exposed to all participants in the global BGP fabric.
- Planning for resilience and responding during a disruption require collating information across multiple infrastructure providers and even multiple infrastructures. In the United States and many other advanced countries, legal obstacles discourage the sharing of information necessary to craft informed responses [65].

As described in Sections 5 and 6, preparing and planning for national-scale resilience must take these factors into account.

4.3 Applying Resilience to Cyber Infrastructure

The MITRE framework defines 14 practices that an enterprise can apply to achieve resilience goals [10]. Some of the practices must be adapted to apply at the national scale whereas other practices are directly applicable. Tables 8 and 9 list the 14 practices and identify the goals for which they are effective.

For each of the 11 applicable practices in Tables 8 and 9, national resilience requires one or more measures to inform investment direction and readiness estimates.

4.4 Measuring Practices in Cyber Infrastructure

For each of the applicable practices, effective resilience requires viable measures. Measures suitable at the national scale are proposed based

Table 8. Resilience practices and national scale.

Practice	**Application**	**Remarks**
Adaptive Response	Withstand, Recover	Adapting to disruptions and degradation is central to withstanding and recovery. At the national scale, adaptive response can use assets/resources from multiple providers.
Analytic Monitoring	Anticipate, Withstand, Recover, Evolve	All the resilience goals depend on the visibility and cross-provider understanding of the operational state of the cyber infrastructure.
Coordinated Defense	Anticipate, Withstand (Adapted)	Coordinated defense must be adapted to the differing authorities of providers, customers and government stakeholders.
Deception		Deception is impractical to apply at the national scale – multi-party operation of the national cyber infrastructure precludes deceiving other parties.
Diversity	Anticipate, Withstand, Recover, Evolve	Infrastructure providers embody diversity at the national scale, but it is a byproduct of diverse business models and history. Resilience requires diversity to be applied intentionally and with measures of provider independence.
Dynamic Positioning	Anticipate, Withstand, Recover	Anticipation entails pre-identification of assets to mitigate disruptions dynamically. Withstanding and recovery require substitutions of alternative capacity for the impacted services.
Dynamic Representation	Anticipate, Withstand	Requires building and maintaining accurate representations of infrastructure elements and their interactions to identify nascent disruptions and inform response activities.
Non-Persistence		Requires operating various portions of the cyber infrastructure in ephemeral and shifting ways, but this can be impractical at the national scale.
Privilege Restriction	Anticipate, Withstand (Adapted)	Privilege restriction must be adapted to apply at the national scale. Instead of managing entity privileges in enterprises, trust relationships must be managed between enterprises, providers and government authorities.

in part on the metrics described in [56] and its references, especially the detailed work by Allen and Curtis [2].

Table 9. Resilience practices and national scale (continued).

Practice	Application	Remarks
Realignment	Anticipate, Recover, Evolve	Realignment of resources, assets and capacity are central to preparing for disruptions and adapting operations after disruptions. But realignment must be informed by effective monitoring and analysis.
Redundancy	Anticipate, Withstand	Redundancy is the provisioning of additional assets or capacity to prepare for disruptions.
Segmentation	Anticipate, Withstand, Recover	At regional and national scales, segmentation entails preparing and activating mechanisms to isolate disrupted infrastructure segments in order to minimize cascading impacts and manage recovery activities. Intentional segmentation across multiple services and providers is very challenging.
Substantiated Integrity	Anticipate, Withstand, Recover	Substantiated integrity becomes the foundation of trust for cooperative planning, response and, especially, recovery.
Unpredictability		Complexity of multi-party infrastructure offers some degree of unpredictability. Intentionally introducing unpredictability may be impossible to coordinate at the national scale.

Adaptive Response. In the foundational services and compute and storage services layers, measures must include an ability to replace or supplement a degraded service with a redundant asset or a substitute, the delay time after decision that the response becomes usable (latency of effective restoration) and the capacity of the redundant or substitute (service load that the substitute can provide). During the anticipate stage, these measures can be quantified through simple testing and exercises, but they apply during the withstand and recover stages.

In the telecommunications and networking layer, adaptive response includes two types of actions. The first type of actions include the ability to block, throttle or render harmless the specific traffic or transactions that cause the disruption. Measures for this include the breadth of coverage (elements of the infrastructure that are covered by the ability (Table 2)), precision of the response action (how selectively blocking or throttling can be applied), consistency of response (whether all the

telecommunications providers apply similar blocking or throttling) and the time delay from decision to effective imposition of the response.

The second type of actions entail the ability to utilize redundant or alternative network capacity to recover from a disruption or destruction. Individual telecommunications carriers possess this ability today, but for national-scale resilience abilities are needed that span the carriers serving each region. The measures include the capacity of redundant assets, coverage that carriers can offer in using the capacity (geographic distribution of the redundancy, especially the identification of locations that lack redundant capacity) and time delay between decision to employ redundant or alternative capacity and effective service recovery.

Analytic Monitoring and Dynamic Representation. The analytic monitoring and dynamic representation practices are separate in the MITRE framework, but need to be planned together in a national-scale resilience effort. A dynamic representation can only be created by monitoring and monitoring at large scales is useful only when processed into an actionable and timely representation. A common, aggregated dynamic representation is a form of shared situational awareness that is identified as important in several large-scale cyber security strategy studies [26, 38].

The analytic monitoring and dynamic representation practices apply to all four resilience stages.

In the foundational services layer, the practices must include fine-grained monitoring and fusion into an actionable representation of service availability and accuracy. However, in this layer, it is especially important that the monitoring include observations of foundational service availability from different national regions and extra-national regions, and comparisons of service-reported data with ground truth samples in order to detect integrity compromises. The measures in this layer include the coverage of elements and service providers, ability to distinguish independent service failures, timeliness of updating the national-scale dynamic representation and accuracy of characterization of service degradation (failure rates, latency, completeness of responses).

In the compute and storage services layer, measures must cover fine-grained monitoring and collation of monitoring data into an accurate high-level picture of service availability and integrity. The measures include the coverage of the monitoring (percentage of provider storage and compute assets monitored), timeliness of updating the national-scale dynamic representation and accuracy of the mapping between monitored assets and overall service posture.

The telecommunications and networking layer must be monitored and represented with exceptional fidelity because all other services and recovery mechanisms depend on the layer. Telecommunications and network carriers already perform a great deal of analytic monitoring, but at this time there is no national-scale effort to build a faithful dynamic representation of network service posture from the data. Creating such a representation is a vital requirement for informing a national-scale resilience effort. The measures in this layer include the independence of the elements comprising the layer, monitoring coverage across carriers, regions and service types (voice, IP traffic, other data traffic, SMS, etc.), timeliness of updating the national-scale dynamic representation and accurate characterization of the capacity of each major asset that provides key services. It does little good to know that an inter-regional link is carrying 5 Gbps of traffic unless the representation also includes the fact that the link capacity is 100 Gbps.

Dynamic representation in all the layers must also have the ability to represent mitigation and recovery response in progress.

Coordinated Defense. Significant research has focused on information sharing for enhancing situational awareness and helping individual defenders coordinate responses; interested readers are referred to [38] for a survey of the literature on situation awareness. Much of the work assumes that coordination is among independent enterprises, each making its own decisions to defend its assets. Such independently-motivated actions that lack common objectives will not achieve resilience at the national scale. Therefore, the coordinated defense practice must have a goal (withstanding and recovering from disruptions and attacks nationally) along with measures of success. The primary measures of success are drawn from shared dynamic representation. Coordination of defensive action depends on mechanisms for selecting coordinated response and recovery actions, and on robust means for disseminating the actions to all parties that can execute them.

In the foundational services and compute and storage services layers, coordinated defense largely involves conventional defensive responses such as blocking, quarantining, segmenting and patching implemented in concert. Measures include the coverage of relevant service providers with the means to accept coordinated action instructions and have agreed to do so, time delay between a response decision and application of the action at covered providers, and breadth of response actions included in the coordinated defense repertoire.

In the telecommunications and networking layer, the same measures apply as in the foundational services layer, but an important addi-

tional measure is automation. Some defensive actions can gain broad impacts automatically via global network control systems such as the global BGP routing fabric or the telecommunications signaling system if providers pre-configure trigger mechanisms such as remote triggered BGP black hole filtering [51]. Therefore, a salient measure is the coverage of telecommunications carriers that have pre-configured the mechanisms and have agreed to accept remote coordinated triggers from an authorized source.

Diversity. The MITRE framework and other resiliency engineering strategies identify infrastructure heterogeneity as a means for reducing the impacts of disruptions and attacks. At the national scale, some inherent diversity may be gained from the various providers in the cyber infrastructure layers. However, a diverse set of providers does not guarantee the technological or process diversity needed to reduce impacts. Measures of diversity across different service elements are essential to understand potential impacts; this applies to all service elements and layers. Measures include diversity assessments of several facets of service elements, including service implementation supplier (web server for the web element, mail transfer agent server for the e-mail element and router vendor for the IP routing element), service platform, service protocol and service management system.

Dynamic Positioning and Realignment. Measures for the dynamic positioning and realignment practice must inform the readiness for disruptions and attacks and extent to which dynamic responses to disruptions and attacks can sustain or restore service availability. Note that this practice is different from redundancy because it involves dynamically shifting capacity or realigning assets to ensure a usable or minimally-degraded service profile for a cyber infrastructure layer.

In the foundational services layer, measures include the coverage of service element scope (e.g., extent to which generic compute resources can be enlisted to restore DNS services), capacity of dynamic response as a fraction of the original service capacity, time delay to implement dynamic response and transparency of the dynamically-realigned service compared with the original service.

In the compute and storage services layer, measures include coverage, capacity fraction and time delay as in the case of the foundational services layer. But a measure of prioritization is also needed, specifically, the degree to which dynamically-realigned assets can support the highest priority workloads or stored data during the withstand and recover

stages, and the degree to which dynamically-realigned assets can serve the highest priority workloads or stored data.

In the telecommunications and networking layer, the key measures are capacity and latency. Telecommunications providers already manage the dynamic allocation of network resources, so the measure of capacity must reflect the fraction of the resource that can be dynamically repositioned within a particular element (e.g., shifting switched link capacity from a local customer to transit usage) and between elements (e.g., shifting IP routed capacity from customer IP usage to signaling system usage).

Privilege Restriction. For national scale resilience, the privilege restriction practice applies to privileges extended between providers. For many types of cyber disruptions, trust between service providers can help propagate disruptive and malicious effects. For example, disruptive route hijacking can occur in the global BGP fabric partly because autonomous system owners (mostly carriers) have too much trust in route information received from their peers [14]. In all the cyber infrastructure layers, measures of trust relationships are critical to qualifying and improving resilience.

Two key measures are the ability of service providers to authenticate peers with whom they interact and the extent of trust that providers extend to authenticated peers compared with the minimum trust necessary to provide service. During the withstand stage, an important response action for some services is minimizing the trust that service providers have on each other in order to slow or halt the spread of disruptions. Therefore, an important measure for all service providers must be their ability to consistently and positively alter their trust configurations and the time delays involved in accomplishing the alterations.

Redundancy. The redundancy practice is one of the simplest means to support resilience, but it must be measured to quantify the national ability to withstand disruptions and to recover from them. Also, redundancy can be economically inefficient. A redundant asset requires capital investment and maintenance, but may not generate full returns. Therefore, an investment in redundancy must be intentional and directed to yield maximum resilience benefits.

In the foundational services and compute and storage services layers, measures of redundancy include the simple ratio of available capacity to expected normal load and the time delay involved in bringing redundant capacity into service after a decision is made. Also, there must be some measure of the geographic or provider distribution of the redundant capacity. National resilience requires the ability to employ redundant ca-

pacity across service providers. For example, if one DNS service provider is disabled by a cyber attack, then another provider must be able to serve the affected domains using its redundant capacity. The time delay for recovering DNS service in such a scenario may be considerable.

In the telecommunications and networking layer, redundancy cannot be measured simply by capacity; instead, it must be characterized geographically and topologically. Simple and general measures for this do not appear to exist. Omer et al. [69] have conducted a deep resilience analysis of a critical portion of the global telecommunications infrastructure. The measures researched in the study should be extensible to the characterization of more general networks.

Note that national resilience requires two types of redundancy to be considered. One is internal redundancy, the measure of available extra capacity within a single provider. The other is external redundancy, the measure of extra capacity accessible by shifting the load to other providers.

Segmentation. Segmentation is the partitioning of a network or service layer into disjoint portions with defined and controlled interfaces between them. It enhances resilience because imposing a limiting interface can halt the spread of disruptive effects. At the national scale, carrier boundaries already constitute the first stratum of segmentation. Within a service layer, large providers should further segment their own portions of the infrastructure to reduce the impacts of disruptions targeted at them or propagated from peers. Effective management of trust relationships also contributes to segmentation during the anticipate stage. In the withstand stage, additional segmentation or subdividing of existing segments can limit impacts and simplify subsequent recovery efforts. Measures for segmentation must include the quantification of segmentation (e.g., number of segments and ratio of largest to smallest segment size) and degree of control imposed between segments. Practices for segmenting services at the enterprise level are available [37]. Some of these practices can be extended to the national scale.

Substantiated Integrity. Substantiated integrity is a subtle but critical practice in resiliency engineering – it is the ability for an infrastructure provider, defensive operator or decision maker to trust that a peer or dependency has not been compromised or co-opted by an attacker such that information or requests from the peer can be used as the basis for action. Few options are available for service layers at the national scale. One exception is the IP routing element for which multiple global-scale trust frameworks are defined but not yet implemented [46].

During the anticipate stage, service providers and carriers must pre-establish trust mechanisms. Two such mechanisms have been used successfully at a large scale:

- Authoritative sources identify and designate sources of authoritative information in advance; these can be individuals or systems. During the withstand and recovery stages, peers accept actionable information or requests only from these trusted sources.

- Cryptographic trust is achieved when peers agree to a mechanism for cryptographically substantiating important information and exchange (in advance) the keys and credentials necessary to support the mechanism.

Taken together, the practices listed above offer a means for service providers, carriers and operators that manage the national cyber infrastructure to prepare for disruptions and attacks, withstand them by reducing their duration and severity, recover from adversity and improve over time.

5. Implementing the Resilience Model

This section offers recommendations on implementing national-scale resilience through the application of the practices detailed in Section 4. The implementation steps are divided into a cycle of four phases, prepare, implement, exercise or test, and evaluate.

5.1 Phase 1: Prepare

Before attempting to apply the practices, the parties involved must gather information and establish relationships.

Step 1.1: Map Dependencies. Dependencies between infrastructure elements and providers for each element must be mapped. The technical operation of each element imposes certain dependencies as shown in Figure 3. But the technical dependencies are only a rough guide for enumerating the operational dependencies in a national infrastructure.

Mapping operational dependencies requires information from all the involved providers. For some elements, basic dependencies can be approximated from information that is publicly visible, especially DNS and IP routing. However, for all other elements, dependency information is scattered among the providers of the elements. This information must be gathered by surveying the providers and refreshed regularly.

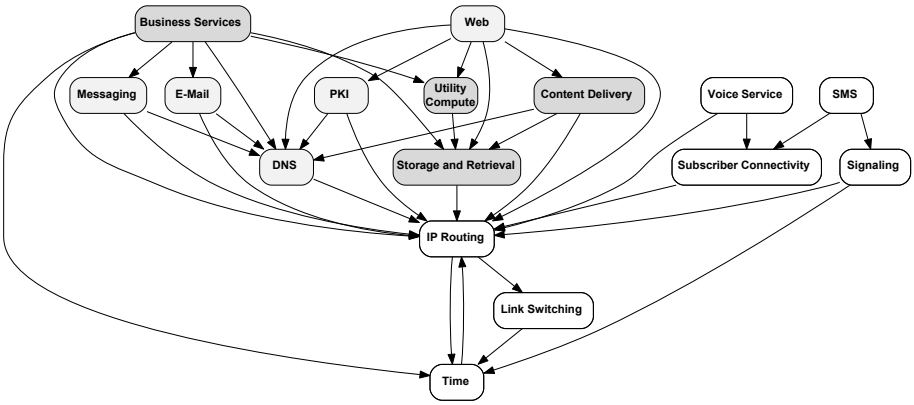

Figure 3. Dependencies between cyber infrastructure elements.

Step 1.2: Assess Key Measures. A critical aspect of preparation is establishing baseline values for critical metrics. In this step, individual providers must assess their infrastructure elements and quantify their postures with respect to each of the practices listed in Section 4. Parties with oversight of infrastructure elements and layers, such as industry sector groups and government agencies, must measure the postures for practices that span multiple providers (e.g., external redundancy and diversity).

Step 1.3: Identify and Build Monitoring and Dynamic Representation Mechanisms. All detection, response and recovery activities depend on the accurate and timely representation of the state of the cyber infrastructure. In this step, responsible parties identify existing monitoring and dynamic representation support, and build new structures where national-scale analysis capacity is lacking.

The monitoring and dynamic representation mechanisms must include data ingestion, processing and delivery of analytic results to automated systems and analysts and decision-makers.

Step 1.4: Identify Key Response and Recovery Tactics. During this step, key stakeholders and service providers enumerate the activities they will employ for particular infrastructure elements and types of disruptions. These include the following practices:

- **Adaptive Response:** Specific response mechanisms are employed to reduce the impacts of disruptions and attacks, including remapping, blackholing, filtering and blacklisting.

- **Coordinated Defense:** Specific defensive measures such as multi-party blocking, redirecting and throttling that providers undertake cooperatively are employed in the event of disruptions and attacks.

- **Dynamic Positioning:** Service loads are shifted between providers or a provider can take on a service burden in support of a disrupted peer.

- **Segmentation:** Additional controlled boundaries between providers or within shared networks are imposed to halt the spread of disruptions.

- **Realignment:** Capacity is realigned from one service to another in order to mitigate a disruption or support recovery.

Step 1.5: Characterize Current Trust Relationships. There are two reasons to enumerate and characterize trust relationships between providers during the prepare phase. First, excessive or unnecessary trust relationships offer malicious actors additional ways to propagate their attacks; these relationships should be minimized as part of the privilege restriction practice. Second, many coordinated defense, realignment and other active responses require trust between participants; all trust relationships that are needed to execute the response and recovery tactics identified in Step 1.4 should be enumerated during this step.

Step 1.6: Identify Mechanisms for Substantiating Integrity. Response and recovery activities, both manual and automated, require that participants are able to trust the information and requests received from service providers and response operators. During this step, mechanisms for establishing and maintaining trust must be selected, characterized and accepted by participants.

5.2 Phase 2: Implement

National resilience stakeholders are responsible for setting up mechanisms and assets for resilience before large-scale disruptions and attacks. This phase includes the major facets of the implementation.

Step 2.1: Establish Response and Recovery Trust Relationships. In this step, infrastructure providers and decision makers set up trust relationships that support the exchange of information for maintaining dynamic representation and coordinating response and recovery activities.

Step 2.2: Initiate Monitoring and Representation. After the trust relationships have been set up, providers can initiate data flows that support the analytic monitoring and dynamic representation practices. Stakeholders responsible for operating the analyses that drive dynamic representation must set up their systems during this step.

Step 2.3: Define Segmentation Boundaries for Response. The segmentation practice can be very effective at bounding the impacts of disruptions and attacks. However, imposing new segmentation requires prior identification of the candidate points at which new interface controls can be placed. During this step, providers in a layer cooperate to identify the candidate points and applicable mechanisms.

Step 2.4: Provision Substantiated Integrity Mechanisms. In this step, providers implement the substantiated integrity practice by provisioning keys, credentials, authoritative sources and other mechanisms defined in Step 1.6. This may include configuring automated systems and protocols, and exchanging lists of designated trusted individuals and their contact information.

Step 2.5: Establish Mechanisms for Key Response and Recovery Tactics. For each of the response and recovery actions identified in Step 1.4, providers pre-provision, document and configure necessary systems and processes for conducting the actions. These include manual processes that must be documented and automated processes that may need to be scripted or installed on operational infrastructure components. This step also includes configuring fail-over and load-shifting mechanisms for utilizing redundant capacity or realigning capacity to service recovery.

Step 2.6: Minimize Trust Relationships. In the last implementation step, providers implement the privilege restriction practice – minimizing external trust relationships to those necessary for normal operations and resilience response.

5.3 Phase 3: Test

This phase is essential to effective response and recovery operations when a national cyber infrastructure is under genuine threat. Testing and exercising responses and recovery actions are a standard part of continuity of operations and disaster recovery readiness [79] and are critical to resilience operations. To facilitate resilience at the national scale,

where multiple private and public sector stakeholders must cooperate to respond and recover, conducting exercises is even more important.

Step 3.1: Hold Tabletop Exercises. As an initial, low-overhead test of response and recovery tactics, key stakeholders should hold simulated manual exercises. These tabletop exercises would not involve real systems or services, but instead rehearse and debug response processes, responsibilities and inter-party relationships. Guidance for running such exercises, albeit in somewhat different contexts, is available from multiple sources [24, 41, 88].

Step 3.2: Test Monitoring and Dynamic Representation. The stakeholders must test monitoring and dynamic representation facilities to ensure that they deliver accurate and actionable information. In this step, providers collaborate with each other and with decision makers to gain assurance. There are several ways to test monitoring systems, but a simple approach that works at any scale is to perturb service functioning either by taking some capacity out of service or applying an artificial service load, and then check that the dynamic representation accurately tracks the actual service posture.

Step 3.3: Test Response and Recovery Actions Internally. This step is performed separately and independently by each provider. It involves testing the internal mechanisms for adaptive response, dynamic positioning, segmentation and other practices. This is an essential step because proper functioning of the independent mechanisms must be assured individually before a national response attempts to use many of them in a concerted fashion.

Monitoring individual tests also offers further opportunities to test monitoring and dynamic representation.

Step 3.4: Test Multi-Party Response and Recovery Actions. This step is very complex, but it is a critical aspect of testing. Providers and decision makers cooperate to test the response and recovery tactics identified in Step 1.4. Tests must include the following facets:

- Application of practices at all providers concurrently.
- Selective application of practices (e.g., blocking or throttling at a subset of providers).
- Staged or sequential application of practices.
- Application of practices when subsets of providers are unable to act.

- Application of multiple independent practices concurrently (e.g., shifting loads to redundant capacity while simultaneously throttling attack traffic).

- Ceasing the application of practices (i.e., testing the actions performed after disruptions as part of return to normal operations).

Step 3.5: Hold Large Scale Functional Exercises. After the dynamic representation is shown to be accurate and individual practices have been tested, the final step is to hold simulation exercises using real infrastructure. These exercises should be confined to individual layers initially to reduce the likelihood of unplanned impacts to service users. Guidance for planning such exercises is available from the National Institute of Standards and Technology (NIST) [41].

5.4 Phase 4: Evaluate

In this phase, the findings from Phases 2 and 3 are compiled and used to characterize gaps, issues and improvements.

Step 4.1: Assess Dynamic Representation. This step evaluates the accuracy and timeliness of the infrastructure state shown by the dynamic representation. Missing elements, excessive time lag and desynchrony, and inaccurate analyses are all opportunities for improvement.

Step 4.2: Assess Operation of Response and Recovery Tactics. During Phase 3, service providers test response and recovery mechanisms, first internally and then cooperatively. All the measures listed in Section 4 can be captured, or at least approximated, during the tests. It is especially important to identify situations where practices can be applied and where applications of different practices conflict.

Step 4.3: Assess Responsibilities and Relationships. Because national cyber resilience depends on the cooperation of many parties, the working relationships between the parties are vital to effective response and recovery. In this step, stakeholders must use the findings from exercises and tests to identify missing relationships and areas that lack clear lines of responsibility.

Practical Considerations Implementing national cyber infrastructure resilience will vary across nations. Several considerations affect how resilient operation can be built up and how response and recovery practices can be managed.

First, the centralization and ownership of infrastructure affects implementation. Highly-centralized services present fewer obstacles to new policies and controls, but offer less inherent diversity, redundancy and segmentation. Decentralized services offer the potential for better inherent support of resilience practices, but require reliable distributed control and associated trust relationships to be built. It is productive to compare the centralized approach taken by Estonia after the attacks against its national cyber infrastructure in 2011 [23] with the decentralized approach proposed for Canada's diverse financial sector in 2014 [39].

Ownership models also impact implementation. Private owners of service infrastructure are driven by business motives, including competitiveness, efficiency and fiduciary obligations to shareholders. Public owners may be responsible for public good, but may lack competitive incentives. In the case of multiple service providers under private ownership, competition concerns can prevent the adoption of resilience practices unless obligations are uniform and consistent (i.e., retain a level playing field).

Regulation can be used to impose requirements on certain behaviors and investments, especially for measures that are easy to quantify such as redundant capacity. Economic incentives such as investment credits and tax reductions can also nudge private sector cyber infrastructure providers to implement resilience practices. Incentive strategies have been advocated in various national policy study reports [19, 71]. However, these incentives must be carefully selected to drive resilience practices that need improvement. Also, incentives leave decision making to infrastructure owners on whether or not to implement a resilience practice; some may choose to forego the incentive.

National cyber resilience absolutely requires information sharing and cooperation among the infrastructure providers that serve the nation. In nations with private ownership of cyber infrastructure, the providers are business competitors. Some nations, especially the United States and several European Union members, impose legal barriers to cooperation among competitors [65]. When these legal barriers can be reduced, information sharing can improve, but other challenges remain [52].

Finally, resilient operation at the national scale requires aggregated visibility (dynamic representation practice) as well as coordinated control (adaptive response, realignment, coordinated defense and other practices). The breadth of the cyber infrastructure and the presence of complex dependencies (Figure 3) imply that no single provider has an incentive to accept responsibility for such visibility and control. The role will fall to the government in some way, either directly as in the United

Kingdom [19] or via some form of government coordination and support as in models proposed for the United States [71].

6. Stakeholders and Roles

The cyber infrastructure of the United States offers excellent opportunities to implement resilience, but legal and economic factors impose substantial challenges.

6.1 Cyber Resilience Government Stakeholders

The first aspect of U.S. national governance that affects cyber infrastructure operation is the number and diversity of government organizations and government-sponsored organizations that share responsibility for cyber issues. Excellent, but security-focused, overviews of this topic appear in the U.S. national plan for cyber incident response [89], in a legal analysis for Congress [75] and in a NATO assessment of the United States as a member [70]. Tables 10 and 11 provide details about the main U.S. Government stakeholders.

In addition to federal authorities, state and territorial governments have regulatory power over some infrastructures in domains, especially subscriber connectivity services.

The key responsibility for cyber infrastructure resilience belongs to the Critical Infrastructure Security Agency, a U.S. Department of Homeland Security entity. However, the telecommunications and information technology sectors, for which CISA is the sector-specific agency, are very large and complex. To foster intra-sector cooperation on cyber matters and to streamline cooperation with the federal government, each sector has an Information Sharing and Analysis Center (ISAC).

- The Communications ISAC is the coordination body responsible for the telecommunications and network infrastructure layer. It is located within CISA as the National Coordinating Center for Communications (NCCC).

- The Information Technology ISAC is the coordination body for the information technology industry, including information technology enterprises and some service providers. Its members cover a portion of the foundational services and compute and storage services layers.

Of the seven service areas in the telecommunications and networking layer, all are represented to a significant degree by the NCCC or an aligned government organization. However, of the nine service areas

Table 10. Main U.S. Government cyber infrastructure stakeholders.

Organization	Description
U.S. Department of Homeland Security (DHS)	Primary responsibility for critical infrastructure protection and cyber incident response with the U.S. Department of Defense, National Security Council Cyber Response Group and sector-specific agencies [66, 68].
Critical Infrastructure Security Agency (CISA)	New agency under DHS (2018) whose responsibilities were located in DHS. Responsible for incident response in federal and critical infrastructure networks. Responsibilities include infrastructure resilience and serving as the sector-specific agency for the telecommunications and information technology sectors [66].
U.S. Department of Defense (DoD)	Responsible for national defense, including defending U.S. territory from foreign threats (Title 10 USC). Several DoD organizations have specific cyber-related authorities. May support any civilian agency in this list under the Defense Support to Civil Authorities Directive [87].
U.S. Cyber Command (USCC)	Unified combatant command under the DoD. Responsible for defending DoD networks and infrastructure, and the national infrastructure when commanded to do so by the U.S. President.
National Security Agency (NSA)	Delegated responsibility for protection and defense of national security systems under National Security Directive 42 [13]. May provide technical support to any federal agency under a Request for Technical Assistance under Executive Order 12333.
National Security Council (NSC)	Maintains oversight of all national security matters, including homeland security and critical infrastructure. Chairs the Cyber Response Group and may convene Cyber Unified Coordination Groups.
Cyber Threat Intelligence Integration Center (CTIIC)	Responsible for providing coordinated intelligence on cyber threats as part of the U.S. Intelligence Community [67].

in the foundational services and compute and storage layers, few are represented by the publicly-disclosed members of the IT-ISAC [48].

To conduct the resilience steps outlined in Section 5, engagement through the IT-ISAC and NCCC are necessary but possibly not suffi-

Table 11. Main U.S. Government cyber infrastructure stakeholders (continued).

Organization	Description
Federal Bureau of Investigation (FBI)	Primary responsibility for investigating and prosecuting cyber crime.
National Cyber Investigative Joint Task Force (NCIJTF)	Established in 2008 as a partnership of 20 federal agencies that cooperate on cyber threat investigations and incident response.
National Institute of Standards and Technology (NIST)	Provides cyber security and cyber risk guidance to the public and private sectors. Under legal authority [67], develops standards to reduce the risk of cyber attacks to critical infrastructure [85]. Also responsible for standards and metrology and supports the global time infrastructure.
Federal Communications Commission (FCC)	Responsible for regulating interstate communications, including portions of the telecommunications and networking layer.

cient. Additional engagement is necessary to ensure participation by the largest providers of the Domain Name System, Web, messaging, public key infrastructure, utility compute, storage, retrieval and backup, and content delivery. Each of these service areas has a different mix of private sector providers:

- **Domain Name System:** Small number of large service providers support multiple top-level domains with the assistance of a large number of registrars. Also includes some major cloud providers.
- **Web:** Large number of service providers of all sizes offering various business models. Also includes most major cloud providers.
- **Messaging:** Most major cloud providers as well as specialist providers in various industry verticals.
- **Public Key Infrastructure:** Small number of major certificate authority providers, including some major cloud providers.
- **Utility Compute:** A few large providers, including most cloud providers, along with an ecosystem of medium-sized and smaller specialty companies.

- **Storage, Retrieval and Backup:** Major cloud providers along with a wide range of specialty providers.
- **Content Delivery:** A few large providers, including most major cloud providers.

The size and variety of the provider space presents challenges to establishing comprehensive analytic monitoring and associated dynamic representations. However, a small number of large cloud providers dominate the U.S. market [28]. Enlisting the cooperation of these dominant private sector companies would provide substantial coverage of the U.S. cyber infrastructure.

6.2 Building Cyber Infrastructure Resilience

The nature of the cyber infrastructure ecosystem and legal and regulatory environments in the United States implies that any campaign to boost resilience would require broad public and private sector cooperation. Each type of entity has different strengths and must assume different roles as described in U.S. Presidential Policy Directive 21 [66] because the resilience of critical infrastructure is a shared responsibility.

The U.S. Federal Government responsibilities include:

- Overall drive and structure of the resilience effort.
- Legal framework for cooperation.
- Economic and regulatory incentives [71].
- Clearinghouse for situational awareness driven by analysis and dynamic representation.
- Intelligence and law enforcement backing for threat warning and deterrence [26].
- Foundations for cross-provider trust relationships.
- Cross-layer and cross-service coordination.

The U.S. infrastructure provider responsibilities include:

- Participation in the resilience engineering and operations campaigns.
- Instrumentation of their own portions of the cyber infrastructure.
- Provisioning and sustaining redundancy.

- Analytic monitoring and timely contributions to the national dynamic representation.
- Cooperation in response and recovery activities.
- Participation in cross-provider trust relationships.
- Engagement in cross-provider redundancy and dynamic repositioning measures.
- Implementation of substantiated integrity measures.

Various U.S. Government agencies, such as the Defense Information Systems Agency (DISA) and NIST, are infrastructure providers. As such, they would be responsible for the same activities as their private sector counterparts.

With the responsibility structure outlined above, the implementation of national cyber resilience in the United States could be achieved in phases, starting with key services on which all the others depend and expanding to the other services. Lessons learned in this phase, especially in Steps 4.1 through 4.3, can be used to guide relevant regulation and investment.

Phase 1. This initial phase should focus on the three telecommunications and networking elements on which all the other cyber infrastructure elements depend, IP routing, link switching and time. The designated sector-specific agencies, especially CISA and FCC, must identify and assemble the service providers with the greatest capacity and largest customer base while also ensuring geographic and sector coverage. NIST should also be involved because it is the ultimate time authority in the United States. After the key providers are assembled, CISA should lead them through the steps described in Section 5, concentrating on applying the resilience practices and testing for the three telecommunications and networking elements.

Phase 2. In Phase 2, the scope of the resilience effort must be expanded to cover all the telecommunications and networking layer elements along with DNS, the foundational services layer element on which most other elements depend. CISA would also lead this phase, but it would engage the DoD because it is the operator of one of the DNS root servers and a top-level DNS domain (`.mil`).

The scope of this phase is quite broad because it covers eight service elements. As a result, it would not be possible to conduct comprehensive tests of attack and disruption scenarios.

Test and exercise scenarios should be drawn from two sources. Leading service providers should provide disruption scenarios based on historical observations. CTIIC should provide attack scenarios based on intelligence assessments of the capabilities, plans and intentions of hostile entities.

The service providers engaged in Phase 2 would include all the providers engaged in Phase 1, along with other telecommunications and networking providers based on their capacity and coverage of subscriber connectivity, signaling, voice service and SMS elements. Finally, major DNS service operators would need to be engaged. The critical activity in Phase 2 is testing dynamic representation, coordinated defense, adaptive response and other resilience practices that span multiple service elements. An example is mitigating a DNS disruption by coordinating IP routing response actions with participating IP routing providers.

Phase 3. In the final phase, resilience engineering practices must be applied to all the service elements in all three layers. Primary considerations during this phase include the accuracy and completeness of the dynamic representation, effectiveness and timeliness of dynamic repositioning and realignment practices, and efficiency of cooperative industry and government response actions. A critical type of testing to be conducted in Phase 3 is the recovery of high-level services (e.g., from the compute and storage services layer) through actions taken in the lower layers.

7. Conclusions

Modern society depends on cyber infrastructure for economic, social and national security. Recent history has shown that cyber infrastructure disruptions and attacks cannot be ignored. Any nation that wishes to continue to enjoy the benefits of its cyber infrastructure must have the ability to withstand disruptions and attacks, and recover from them. At the national scale, the only way to ensure this ability is to build resilience into the cyber infrastructure and establish trust and cooperative relationships between private sector infrastructure operators and responsible government entities.

This paper has presented several suggestions for improving cyber infrastructure resilience at the national scale. But several open issues will present challenges to achieving a robust implementation. Some of the issues are technical in nature and should be resolved through conventional research. The biggest challenge is applying resilience engineering to a diverse and evolving cyber infrastructure, especially when the components of the infrastructure often cross-national boundaries. However,

the reliance and dependence on cyber infrastructure will not permit inaction because the potential impacts of disruptions and attacks to national security, prosperity and societal well-being are just too great.

References

[1] F. Alaba, M. Othman, I. Hashem and F. Alotaibi, Internet of Things security: A survey, *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

[2] J. Allen and P. Curtis, Measures for Managing Operational Resilience, Technical Report CMU/SEI-2011-TR-019, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, 2011.

[3] B. Amann, R. Sommer, M. Vallentin and S. Hall, No attack necessary: The surprising dynamics of SSL trust relationships, *Proceedings of the Twenty-Ninth Annual Computer Security Applications Conference*, pp. 179–188, 2013.

[4] M. Amin, Challenges in reliability, security, efficiency and resilience of energy infrastructure: Towards a smart self-healing electric power grid, *Proceedings of the IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century*, 2008.

[5] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, A view of cloud computing, *Communications of the ACM*, vol. 53(4), pp. 50–58, 2010.

[6] M. Assuncao, R. Calheiros, S. Bianchi, M. Netto and R. Buyya. Big data computing and clouds: Trends and future directions, *Journal of Parallel and Distributed Computing*, vol. 79-80, pp. 3–15, 2015.

[7] D. Atkins and R. Austein, Threat Analysis of the Domain Name System (DNS), RFC 3833, 2004.

[8] D. Atkins, K. Droegemeier, S. Feldman, H. Garcia-Molina, M. Klein, D. Messerschmitt, P. Messina, J. Ostriker and M. Wright, Revolutionizing Science and Engineering Through Cyberinfrastructure: Report of the National Science Foundation Blue-Ribbon Advisory Panel on Cyberinfrastructure, Alexandria, Virginia (`www.nsf.gov/cise/sci/reports/atkins.pdf`), 2003.

[9] T. Aven, On some recent definitions and analysis frameworks for risk, vulnerability and resilience, *Risk Analysis*, vol. 31(4), pp. 515–522, 2011.

[10] D. Bodeau and R. Graubart, Cyber Resiliency Engineering Framework, Technical Report MTR110237, MITRE Corporation, Bedford, Massachusetts, 2011.

[11] A. Boin and A. McConnell, Preparing for critical infrastructure breakdowns: The limits of crisis management and the need for resilience, *Journal of Contingencies and Crisis Management*, vol. 15(1), pp. 50–59, 2007.

[12] T. Brooks, *Cyber-Assurance for the Internet of Things*, IEEE Press, Piscataway, New Jersey, 2017.

[13] G. Bush, National Security Directive – National Policy for the Security of National Security Telecommunications and Information Systems, National Security Directive 42, The White House, Washington, DC, July 5, 1990.

[14] K. Butler, T. Farley, P. McDaniel and J. Rexford, A survey of BGP security issues and solutions, *Proceedings of the IEEE*, vol. 98(1), pp. 100–122, 2010.

[15] A. Chakrabarti and G. Manimaran, Internet infrastructure security: A taxonomy, *IEEE Network*, vol. 16(6), pp. 13–21, 2002.

[16] B. Clinton, Executive Order 13010 – Critical infrastructure protection, *Federal Register*, vol. 61(138), pp. 37345–37350, 1996.

[17] D. Comer, *The Internet Book: Everything You Need to Know About Computer Networking and How the Internet Works*, CRC Press, Boca Raton, Florida, 2019.

[18] T. Comes and B. Van de Walle, Measuring disaster resilience: The impact of Hurricane Sandy on critical infrastructure systems, *Proceedings of the Eleventh International ISCRAM Conference*, pp. 190–199, 2014.

[19] P. Cornish, R. Hughes and D. Livingstone, Cyberspace and the National Security of the United Kingdom: Threats and Responses, A Chatham House Report, Chatham House, London, United Kingdom, 2009.

[20] D. Crocker, Internet Mail Architecture, RFC 5598, 2009.

[21] G. Cybenko, Quantifying and measuring cyber resiliency, *Proceedings of SPIE*, vol. 9825, pp. 98250R-1–98250R-6, 2016.

[22] Cyber Security and Infrastructure Security Agency, Critical Infrastructure Sectors, Arlington, Virginia (`www.dhs.gov/cisa/critical-infrastructure-sectors`), 2020.

[23] C. Czosseck, R. Ottis and A. Taliharm, Estonia after the 2007 cyber attacks: Legal, strategic and organizational changes in cyber security, *International Journal of Cyber Warfare and Terrorism*, vol. 1(1), pp. 24–34, 2011.

[24] D. Dausey, J. Buehler and N. Lurie, Designing and conducting tabletop exercises to assess public health preparedness for manmade and naturally-occurring biological threats, *BMC Public Health*, vol. 7, article no. 1, 2007.

[25] K. de Leeuw and Jan Bergstra (Eds.), *The History of Information Security: A Comprehensive Handbook*, Elsevier, Amsterdam, The Netherlands, 2007.

[26] Defense Science Board, Task Force Report: Resilient Military Systems and the Advanced Cyber Threat, U.S. Department of Defense, Washington, DC, 2013.

[27] D. Denning, Activism, hacktivism and cyberterrorism: The Internet as a tool for influencing foreign policy, in *Networks and Netwars: The Future of Terror, Crime and Militancy*, J. Arquilla and D. Ronfeldt (Eds.), RAND Corporation, Santa Monica, California, pp. 239–288, 2001.

[28] L. Dignan, Top cloud providers 2019: AWS, Microsoft Azure, Google Cloud; IBM makes hybrid move; Salesforce dominates SaaS, *ZDNet*, August 15, 2019.

[29] T. Dillon, C. Wu and E. Chang, Cloud computing: Issues and challenges, *Proceedings of the Twenty-Fourth IEEE International Conference on Advanced Information Networking and Applications*, pp. 27–33, 2010.

[30] C. Doerr and F. Kuipers, All quiet on the Internet front? *IEEE Communications*, vol. 52(10), pp. 46–51, 2014.

[31] M. Dunn Cavelty, Critical information infrastructure: Vulnerabilities, threats and responses, *UNIDIR Disarmament Forum*, vol. 2007(3), pp. 15–22, 2007.

[32] M. Elgazzar, Perspectives on M2M protocols, *Proceedings of the Seventh IEEE International Conference on Intelligent Computing and Information Systems*, pp. 501–505, 2015.

[33] Executive Office of the President, National Security Strategy of the United States of America, The White House, Washington, DC, 2017.

[34] M. Faloutsos, P. Faloutsos and C. Faloutsos, On power-law relationships of the Internet topology, *ACM SIGCOMM Computer Communication Review*, vol. 29(4), pp. 251–262, 1999.

[35] Federal Communications Commission, Annual Report and Analysis of Competitive Market Conditions with Respect to Mobile Wireless, Nineteenth Report, Washington, DC, 2016.

[36] T. Fleury, H. Khurana and V. Welch, Towards a taxonomy of attacks against energy control systems, in *Critical Infrastructure Protection II*, M. Papa and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 71–85, 2008.

[37] J. Frahim and A. Raza, A Framework to Protect Data Through Segmentation, Cisco Systems, San Jose, California (`www.cisco.com/c/en/us/about/security-center/framework-segmentation.html`), 2019.

[38] U. Franke and J. Brynielsson, Cyber situational awareness – A systematic review of the literature, *Computers and Security*, vol. 46, pp. 18–31, 2014.

[39] H. Gallagher, W. McMahon and R. Morrow, Cyber security: Protecting the resilience of Canada's financial system, *Bank of Canada Financial System Review*, vol. 2014, pp. 47–53, 2014.

[40] K. Geers, The cyber threat to national critical infrastructures: Beyond theory, *Information Security Journal: A Global Perspective*, vol. 18(1), pp. 1–7, 2009.

[41] T. Grance, T. Nolan, K. Burke, R. Dudley, G. White and T. Good, Guide to Test, Training and Exercise Programs for IT Plans and Capabilities, NIST Special Publication SP 800-84, National Institute of Standards and Technology, Gaithersburg, Maryland, 2006.

[42] E. Gregori, A. Improta, L. Lenzini and C. Orsini, The impact of IXPs on the AS-level topology structure of the Internet, *Computer Communications*, vol. 34(1), pp. 68–82, 2011.

[43] J. Hernandez-Castro, E. Cartwright and A. Stepanova, Economic Analysis of Ransomware, arXiv: 1703.06660 (`arxiv.org/pdf/1703.06660.pdf`), 2017.

[44] R. Housley and T. Polk, *Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure*, John Wiley and Sons, New York, 2001.

[45] C. Huitema, *Routing in the Internet*, Prentice Hall, Paramus, New Jersey, 1999.

[46] G. Huston, M. Rossi and G. Armitage, Securing BGP – A literature survey, *IEEE Communications Surveys and Tutorials*, vol. 13(2), pp. 199–222, 2011.

[47] IDG Communications, 2018 Cloud Computing Survey, Needham, Massachusetts, 2018.

[48] Information Technology – Information Sharing and Analysis Center, IT-ISAC Membership, Manassas, Virginia (`www.it-isac.org/members`), 2022.

[49] R. Jennings, E. Nahum, D. Olshefski, D. Saha, Z. Shae and C. Waters, A study of Internet instant messaging and chat protocols, *IEEE Network*, vol. 20(4), pp. 16–21, 2006.

[50] D. Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, Scribner, New York, 1996.

[51] T. King, C. Dietzel, J. Snijders, G. Doering and G. Hankins, BLACKHOLE Community, RFC 7999, 2016.

[52] N. Kshetri, Recent U.S. cybersecurity policy initiatives: Challenges and Implications, *IEEE Computer*, vol. 48(7), pp. 64–69, 2015.

[53] P. Kuhn, C. Pack and R. Skoog, Common channel signaling networks: Past, present, future, *IEEE Journal on Selected Areas in Communications*, vol. 12(3), pp. 383–394, 1994.

[54] J. Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, Washington, DC, 2002.

[55] T. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, John Wiley and Sons, Hoboken, New Jersey, 2020.

[56] I. Linkov, D. Eisenberg, K. Plourde, T. Seager, J. Allen and A. Kott, Resilience metrics for cyber systems, *Environment Systems and Decisions*, vol. 33(4), pp. 471–476, 2013.

[57] C. Liu and P. Albitz, *DNS and BIND*, O'Reilly Media, Sebastopol, Califormia, 2006.

[58] S. Madnick and J. Donovan, Application and analysis of the virtual machine approach to information system security and isolation, *Proceedings of the ACM Workshop on Virtual Computer Systems*, pp. 210–224, 1973.

[59] S. Mansfield-Devine, The growth and evolution of DDoS, *Network Security*, vol. 2015(10), pp. 13–20, 2015.

[60] O. Michel and E. Keller, SDN in wide-area networks: A survey, *Proceedings of the Fourth International Conference on Software-Defined Systems*, pp. 37–42, 2017.

[61] J. Miriam and R. Kerber, Critical Homeland Infrastructure Protection, Report of the Defense Science Board Task Force on Critical Infrastructure Protection, U.S. Department of Defense, Washington, DC, 2007.

[62] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford and N. Weaver, The Spread of the Sapphire/Slammer Worm, Center for Applied Internet Data Analysis, University of California San Diego, La Jolla, California, 2003.

[63] T. Neagoe, V. Cristea and L. Banica, NTP versus PTP in computer network clock synchronization, *Proceedings of the IEEE International Symposium on Industrial Electronics*, pp. 317–362, 2006.

[64] G. Nibaldi, Proposed Technical Evaluation Criteria for Trusted Computer Systems, Technical Report M79-225, MITRE Corporation, Bedford, Massachusetts, 1979.

[65] A. Nolan, Cybersecurity and Information Sharing: Legal Challenges and Solutions, CRS Report R43941, Congressional Research Service, Washington, DC, 2015.

[66] B. Obama, Presidential Policy Directive – Critical Infrastructure Security and Resilience, Presidential Policy Directive 21, The White House, Washington, DC, February 12, 2013.

[67] B. Obama, Presidential Memorandum – Establishment of the Cyber Threat Intelligence Integration Center, The White House, Washington, DC, February 25, 2015.

[68] B. Obama, Presidential Policy Directive – United States Cyber Incident Coordination, Presidential Policy Directive 41, The White House, Washington, DC, July 26, 2016.

[69] M. Omer, R. Nilchiani and A. Mostashari, Measuring the resilience of the transoceanic telecommunications cable system, *IEEE Systems Journal*, vol. 3(3), pp. 295–303, 2009.

[70] P. Pernik, J. Wojtkowiak and A. Verschoor-Kirss, National Cyber Security Organization: United States, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2016.

[71] President's Commission on Enhancing National Cybersecurity, Report on Securing and Growing the Digital Economy, Executive Office of the President, The White House, Washington, DC, 2016.

[72] A. Rathmell, Cyber-terrorism: The shape of future conflict? *Journal of Financial Crime*, vol. 6(3), pp. 277–283, 1999.

[73] Ribbon Communications, What is Diameter Protocol? Plano, Texas (`ribboncommunications.com/company/get-help/glossary/diameter-protocol`), 2019.

[74] S. Rinaldi, J. Peerenboom and T. Kelly, Identifying, understanding and analyzing critical infrastructure interdependencies, *IEEE Control Systems*, vol. 21(6), pp. 11–25, 2001.

[75] J. Rollins and A. Henning, Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations, CRS Report R40427, Congressional Research Service, Washington, DC, 2009.

[76] F. Sabahi, Cloud computing security threats and responses, *Proceedings of the Third IEEE International Conference on Communication Software and Networks*, pp. 245–249, 2011.

[77] J. Saltzer and M. Schroeder, The protection of information in computer systems, *Proceedings of the IEEE*, vol. 63(9), pp. 1278–1308, 1975.

[78] K. Sivalingam and S. Subramaniam (Eds.), *Optical WDM Networks: Principles and Practice*, Kluwer Academic Publishers, New York, 2000.

[79] S. Snedaker, *Business Continuity and Disaster Recovery Planning for IT Professionals*, Syngress, Waltham, Massachusetts, 2013.

[80] E. Spafford, The Internet Worm incident, *Proceedings of the Second European Software Engineering Conference*, pp. 446–468, 1989.

[81] J. Sterbenz, D. Hutchison, E. Cetinkaya, A. Jabbar, J. Rohrer, M. Scholler and P. Smith, Resilience and survivability in communication networks: Strategies, principles and survey of disciplines, *Computer Networks*, vol. 54(8), pp. 1245–1265, 2010.

[82] C. Stewart, S. Simms, B. Plale, M. Link, D. Hancock and G. Fox, What is cyberinfrastructure? *Proceedings of the Thirty-Eighth Annual ACM SIGUCCS Fall Conference: Navigation and Discovery*, pp. 37–44, 2010.

[83] A. Taylor and J. Vincent, An SMS history, in *Mobile World*, L. Hamill, A. Lasen and D. Diaper (Eds.), Springer, London, United Kingdom, pp. 75–91, 2005.

[84] U.S. Computer Emergency Readiness Team, CERT Advisory CA-2002-03: Multiple vulnerabilities in many implementations of the Simple Network Management Protocol (SNMP), Washington, DC, March 11, 2002.

[85] U.S. Congress, Public Law 113 – 274, Cybersecurity Enhancement Act of 2014, Washington, DC, 2014.

[86] U.S. Department of Defense, Department of Defense Trusted Computer System Evaluation Criteria, Publication DoD 5200.28-STD, Washington, DC, 1985.

[87] U.S. Department of Defense, Defense Support of Civil Authorities (DSCA), Directive 3025.18, Washington, DC, 2010.

[88] U.S. Department of Defense, The Department of Defense Cyber Table Top Guidebook, Version 1.0, Washington, DC, 2018.

[89] U.S. Department of Homeland Security, National Cyber Incident Response Plan, Washington, DC (www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf), 2016.

[90] A. Viswanathan, N. Feldman, Z. Wang and R. Callon, Evolution of multiprotocol label switching, *IEEE Communications*, vol. 36(5), pp. 165–173, 1998.

[91] V. Voydock and S. Kent, Security mechanisms in high-level network protocols, *ACM Computing Surveys*, vol. 15(2), pp. 135–171, 1983.

[92] C. Weissman, Security controls in the ADEPT-50 time-sharing system, *Proceedings of the AFIPS Fall Joint Computer Conference*, pp. 119–133, 1969.

[93] J. Wu, Y. Zhang, Z. Mao and K. Shin, Internet routing resilience to failures: Analysis and implications, *Proceedings of the ACM CoNEXT Conference*, article no. 25, 2007.