In partnership with

CyberRisk ALLIANCE

ICIT

The Institute for Critical Infrastructure Technology (ICIT)

Task Force on Digital Consolidation

Task Force Members

Brett Freedman (CO-CHAIR)
Cory Simpson (CO-CHAIR)
Marene Allison
Edna Conway
Nick Anderson
Ankur Sheth

Foreword

Consolidation is a common thread that runs throughout human history. Time and again, smaller entities—whether civilizations, communities, or companies—have combined to form larger entities driven by the promise of economic, political, or societal gain. We are now witnessing another era of consolidation, one not confined to our physical world, but occurring in the digital world.

The digital world has brought extraordinary beneficial changes to society, connecting us in ways once thought to be unimaginable. These developments have overwhelmingly been for the better, enhancing lives, enabling progress, and resulting in the unprecedented accumulation of wealth. However, as history has shown, consolidation introduces risks alongside rewards. The same unique characteristics of the digital age that make it so valuable—open access, vast concentrations of data, and emergent technologies like artificial intelligence—amplify these risks when critical digital functions and infrastructure are clustered within a small number of private-sector entities. The result is the creation of single points of failure to essential components and functions within our digital infrastructure.

The clustering of these critical functions within the complex and interconnected systems that underpin our digital world has also made it easy for bad actors—nation-states and others—to identify valuable targets as they seek to cause widespread digital disruption.

The growing geopolitical rivalry between the United States and China further exacerbates this risk. The U.S. and Western nations operate in an interconnected, open, and largely privately owned digital ecosystem characterized by the age-old tenets of individual freedom, privacy, and freedom of expression. In contrast, China offers a distinct “digital world” as an alternative. The Chinese model fails to distinguish between public and private entities, reflecting starkly different values of state control, pervasive surveillance, and suppression of dissent.

China’s digital vision is not limited to its borders. It exports its model to other nations, challenging Western digital standards. Simultaneously, China’s struggling domestic economy and aging population create volatility for the governing Chinese Communist Party that could spur their leadership to undertake increasingly aggressive strategies to exploit vulnerabilities in U.S. digital critical infrastructure. This challenge—the rise of a competing digital model espoused by an adversary with both motive and capability—underscores the urgency for the United States to address the risks of digital consolidation. Failure to act renders vulnerable our critical infrastructure and systems, exposing our digital world to widespread disruption in an era of escalating global competition.

Building resilience, the capacity to withstand or recover quickly, in our digital world is imperative when even the most secure systems can be breached by determined adversaries. We must, therefore, prepare for and mitigate the cascading impacts of attacks targeting these consolidated private-sector entities.

This report is not a treatise on the broader sustainability questions of free markets or social contracts, although those discussions must be had. Instead, it’s a call to action for immediate and practical measures to mitigate the societal risks of digital consolidation and ensure the systems underpinning our lives remain resilient.

Our willingness to try to advance this discussion reflects ICIT’s unwavering commitment to modernizing, securing, and strengthening the critical infrastructure that provides for people’s foundational needs.

The Institute for Critical Infrastructure Technology (ICIT)
December 2024

Contents

Executive Summary

Building Resilience to Societal Risk in a Digitally Consolidated World

The digital world has become as vital to modern life as our physical world. What began as a means for communication and entertainment evolved into a domain of commerce, innovation, and diplomacy. Today, our digital world underpins everything from the economy to national security, healthcare, public services, and personal connectivity. However, network effects, structural incentives, and market forces have reduced the number of technologies, companies, and stakeholders building and defending our digital world. This reliance on a consolidated digital ecosystem creates societal risks. To safeguard our future, we must prioritize resiliency and reduce the risk inherent in digital concentration.

This report presents a focused framework to address this urgent challenge by leveraging the

4-Rs of Digital Resilience:

RESOURCING

Market forces alone have failed to drive the investments needed to mitigate the societal risk created by digital consolidation. The U.S. government must, therefore, make targeted and modest investments to facilitate such resilience.

RECOVERY

Preparing for digital disasters caused or exacerbated by consolidation requires a paradigm shift in planning. Just as we prepare for physical disasters by establishing comprehensive recovery plans to restore critical systems, infrastructure, and public confidence following a significant disruption, we must similarly prepare for digital disasters.

REHEARSING

Recovery from a large-scale digital disaster will require cooperation between the public and private sectors at an unprecedented speed and scale. To ensure preparedness, we must rigorously test recovery plans through collaborative exercises involving government and industry. These rehearsals should simulate real-world scenarios, focusing on coordinating efforts, allocating resources, and restoring critical systems efficiently. Such testing is essential to identify gaps and strengthen the cooperative frameworks necessary to mitigate the risks associated with digital consolidation.

RESPONSE

Ambiguity in cyberspace emboldens malicious nation-state and criminal actors. To deter the exploitation of digital consolidation, the U.S. must articulate and enforce clear response policies, making it evident that any successful or attempted attack on the private sector will trigger a decisive response from the U.S. government.

ICIT | CyberRisk ALLIANCE

A Message from the Task Force

The United States faces a significant risk in its digital infrastructure that must be urgently addressed: consolidation. The digital world is unique because it is a good or service as much as a domain of human interaction and existence. As such, it is subject to market realities, and in the United States, markets have long trended toward greater consolidation.[1] Consolidation has occurred across the digital ecosystem, from entities building and maintaining our digital world to those securing and defending it for several reasons:

- Economies of scale,
- Network effects,
- Regulatory environments,
- Access to capital, and
- Technological advancements.

Such consolidation has delivered tremendous benefits to our daily lives, allowing us to take advantage of new products and services at reasonable prices. However, digital consolidation has also created a societal risk[2] that the next administration and Congress must address.

Private sector companies with whom the federal government has consolidated core digital functions are not only easily identifiable targets for nation-states and other bad actors seeking to cause widespread digital disruption but are also vulnerable to the consequences of mistakes or technical failures. Such disruptions could quickly cascade across interconnected systems through malicious intent or inadvertent errors, amplifying their impact on the economy, security, and daily life in the United States.

When we live in a world where we must assume that an entity targeted in cyberspace by a skilled and determined adversary can and will be breached,[3] the U.S. government is obligated to do more with the private sector to ensure resilience from such attacks targeting private-sector consolidators.

The digital world must not be a liability for bad actors to exploit or a societal risk due to technical vulnerabilities and errors. Resilience is no longer an option but a necessity. Actions undertaken by prior Administrations and Congress have made tremendous progress in important areas. Yet, further action by the U.S. government is required to protect our digital world.[4]

THE GEOPOLITICAL RIVALRY BETWEEN THE UNITED STATES AND CHINA AMPLIFIES THE RISK:

- China's relentless cyber and digital consolidation strategies, including state-sponsored attacks and influence campaigns, directly threaten U.S. economic and national security. The United States must decisively counter these threats and secure its digital infrastructure;
- While democratic nations strive to preserve a free, open, and interconnected digital ecosystem, China has constructed a separate digital world designed to reflect its values of control and surveillance;
- This "splinternet" gives China's independent digital infrastructure a higher tolerance for disruption;[5]
- China's domestic decline may also increase its willingness to assume greater geopolitical risk, increasing the stakes for the United States and fellow democracies; and[6]
- China employs cyber operations as a cornerstone of its economic warfare strategy, targeting critical U.S. industries, intellectual property, and infrastructure to gain geopolitical and economic advantage.

Why This Effort?

The term "cyberspace," coined by William Gibson in 1982,[7] once captured our imagination and interest. Today the term falls far short of being able to describe the domain's importance to our way of life. Even Gibson later described cyberspace as an "essentially meaningless" term.[8] Framing our digital world with an opaque, sci-fi-inspired label obscures its critical role. Today, the digital world is as vital as the physical one, underpinning essential systems that ensure societal functionality. For example, the integrity of Electronic Benefits Transfer systems is crucial for distributing food assistance to millions. Any operational degradation of these systems, however brief, can result in significant societal disruptions and deprive or delay essential resources to those most vulnerable.[9] A more alarming example is the cybersecurity of nuclear weapons systems; vulnerabilities could lead to unauthorized access or catastrophic malfunctions.[10] These examples illustrate that the digital world is not merely a realm of exploration or entertainment but a foundation of modern society, demanding the same stewardship that is applied to the physical world.

The risks of digital consolidation are not new,[11] but they are accelerating.[12] Continued market consolidation has created efficiencies and magnified risk by having so many eggs in so few baskets.[13] Cyber incidents have doubled in frequency,[14] and adversaries' capabilities have grown in sophistication. There are fewer targets with far more significant consequences if protections fail or falter. Meanwhile, geopolitical tensions rise. China's partnerships with Russia, North Korea, and Iran increase the likelihood of coordinated and damaging attacks.[15] Building resilience to the societal risk posed by consolidation in our digital world is no longer a distant objective but a pressing necessity that the incoming Administration and Congress must confront.

Our Hope

We present this report with hope and determination. We aim to provide a roadmap to strengthen resilience in the digital world, ensuring our ability to withstand and recover from widespread attacks. Achieving this will require unprecedented collaboration between the federal government and private-sector leaders.

Our recommendations focus on immediate and actionable steps:

- Resourcing redundancy in critical systems to reduce single points of failure and digital resilience efforts more broadly;
- Developing and implementing cohesive and scaled digital disaster recovery plans led by the U.S. government and fully integrated with state, local, tribal, and territorial governments and the private sector;
- Conducting rigorous rehearsals for mass digital disruption scenarios; and
- Sending a clear message to China and others that attempts to exploit the societal risk caused by digital consolidation will be met with significant consequences by the U.S. government.

This report emphasizes the urgent need to prioritize Resourcing, Recovering, Rehearsing, and Responding—the four essential pillars to building resilience in a digitally consolidated world.

Yours in Service,

Marene Allison *Nick Anderson* *Edna Conway*

Brett Freedman (Co-Chair) *Ankur Sheth* *Cory Simpson (Co-Chair)*

Methodology: How the Task Force Approached Its Work

ICIT convened this Task Force in the Summer of 2024 primarily in response to two pivotal events that, taken together, underscored vulnerabilities deriving from digital consolidation:

1. The Cyber Safety Review Board's report in April 2024, and
2. The CrowdStrike outage in July 2024.

These events collectively demonstrated the urgent need to address the risk associated with digital consolidation and the concentration of critical services among a few providers.

The Cyber Safety Review Board's report on the Microsoft Exchange Online Intrusion released in April 2024 highlighted the critical role of cloud computing to the nation and much of the world, as well as what could go wrong when a company, in this case Microsoft, fails to uphold sound security and risk management practices.[16] The report underscored the growing dependence on a small number of cloud service providers (CSPs), making them high-value targets for adversaries and single points of failure in the digital ecosystem.

The July 2024 CrowdStrike outage,[17] triggered by a faulty software update, affected approximately 8.5 million Windows devices—less than one percent of Windows machines worldwide—and cost U.S. Fortune 500 companies an estimated $5.4 billion,[18] demonstrating how even minor disruptions in widely used systems can rapidly cascade across the economy.

These two events highlighted significant vulnerabilities in the digital world of the United States and fellow democratic nations. The incidents galvanized the need to bring together experienced experts and leaders to examine the questions around digital consolidation. ICIT assembled a diverse set of subject matter experts and senior leaders to form a task force to develop actionable recommendations for the next Administration and Congress to address the societal risks posed by digital consolidation.

The ICIT Task Force on Digital Consolidation Risk consists of six members: Marene Allison, Nick Andersen, Edna Conway, Brett Freedman, Ankur Sheth, and Cory Simpson. Each member signed an "Ethics Pledge" to maintain independent thought, confidentiality, neutral and detached recommendations, and adherence to best-practice security protocols.

The ICIT Task Force on Digital Consolidation Risk employed a multifaceted approach. Recognizing the urgency of our task, we assembled our team, identified key areas of focus, and engaged stakeholders across industry, government, academia, civil society, and international partners and allies.

ICIT also partnered with CyberRisk Alliance (CRA) to survey over 300 industry, cybersecurity, and business executives to capture sentiments about digital consolidation. Equipped with this wealth of input, we transitioned to drafting the report, carefully synthesizing information gathered and augmenting it with our collective knowledge and experience to form a cohesive and compelling narrative contextualizing digital consolidation and actionable recommendations tailored for the incoming administration and Congress.

The draft was then rigorously reviewed and refined through expert critiques, allowing us to enhance the clarity and impact of our recommendations. This collaborative and inclusive process culminated in the final publication of the report, ready to inform and guide policy decisions in this critical area.

Tackling the entrenched and multifaceted challenge of digital consolidation required the Task Force to balance urgency with precision, ensuring the final report met the highest standards of rigor. Recognizing the issue's significance, we engaged widely with a diverse set of stakeholders to gather essential perspectives while adhering to a structured, objective methodology. Our efforts were guided by a singular purpose: to provide policymakers with actionable and impactful solutions that address the societal risks of digital consolidation and offer a roadmap for a more secure and resilient digital ecosystem. While this report does not purport to resolve all the complexities of digital consolidation, it represents a critical step toward mitigating its risks and advancing a more resilient digital future.[19]

How We Got Here: History of Digital Consolidation

Consolidation has shaped the digital world from its inception. ARPANET, the precursor to the internet, was a centralized U.S. government project, and IBM's dominance in mainframe computing established the backbone of the modern digital ecosystem. While these early systems enabled the decentralization of users and networks—empowering individuals and democratizing information—they relied on concentrated infrastructure. This paradox, where decentralization thrives atop centralization, remains a defining feature of the digital age.

From IBM's dominance in the 1970s to Microsoft's operating system monopoly in the 1990s to Google's control over online advertising in the 2000s, consolidation has driven innovation, efficiency, and scale. Today, hyperscalers like Amazon, Microsoft, and Google dominate cloud computing, while companies like OpenAI and Anthropic lead in artificial intelligence. These advances have revolutionized connectivity and technology but also introduced systemic risks to stability and resilience.

Understanding this history of digital consolidation is an important step to addressing the challenges it presents. The same infrastructure that connects and empowers society also concentrates risk, where disruptions to a single provider can cascade through interconnected systems, causing widespread disruption. The tension between decentralization and centralization is not an anomaly—it is the core dynamic of our digital evolution and a principle likely to shape its future. To navigate these risks, we must prioritize digital resilience, learning from the past to balance progress with the need for robust and resilient infrastructure.

Advanced Research Projects Agency Network (ARPANET) to the Internet

The beginnings of our digital world can be traced back to the U.S. Department of Defense and the revolutionary concept of "packet switching."[20] The digital era took root in the early 1970s, driven by rapid technological advancements that laid the foundation for today's interconnected systems. In 1972, the ARPANET—an early packet-switched network precursor to the modern Internet—enabled widespread digital connectivity.

These innovations advanced rapidly over the ensuing decades, embedding digital technologies into personal, economic, and governmental domains. By the 1980s, the foundational architecture of a global digital ecosystem had emerged, enabling the widespread adoption of digital communication, processing, and storage that underpin modern life. Crucially, the early internet was built on open protocols that encouraged participation and innovation, allowing a diversity of networks to flourish. This openness remains essential to resilience. On the global internet, if one network becomes unavailable or congested, agreed-upon technical standards ensure that traffic can seamlessly reroute through another. Interoperability is the backbone of this adaptability, sustaining the internet's capacity to endure disruptions and evolve.

Digital Landmarks and Consolidation Trends

As digital technology matured, certain pivotal developments led to the concentration of digital capabilities within a handful of dominant companies. Landmark innovations such as Microsoft's dominance in operating systems, Apple's transformation of personal computing and mobile technology, and Google's supremacy in internet search and digital advertising established what is now often called a "digital monoculture." This trend continued into the 21st century with the rapid growth of the cloud in which Amazon, Microsoft, and Google emerged as dominant players, controlling significant portions of the cloud storage and computing markets.[21]

Key consolidation markers in recent history include:

1970s–1980s

Mainframes

IBM's control over mainframe computing established a foundational infrastructure for enterprise computing. IBM's proprietary hardware and software systems became integral to industries worldwide, consolidating power in critical sectors, including finance, healthcare, and government.[22]

1990s

Operating Systems

Microsoft's dominance over PC operating systems created a uniform landscape where vulnerabilities in Windows could spread widely, exemplifying the security risks of relying on a single provider.[23]

1990s–2000s

Databases

Oracle's rise as the dominant database provider set a precedent for consolidation in enterprise data management. Its systems became indispensable for businesses and governments, locking many institutions into proprietary database solutions.[24]

2000s

Searching and Advertising

Google's dominance in search engines and digital advertising set a precedent for control over data and information access.[25]

2010s

Cloud Computing

Amazon Web Services (AWS), Microsoft Azure, and Google Cloud solidified their positions as the dominant cloud infrastructure providers. They currently control more than 60 percent of the ever-growing cloud market, centralizing critical functions that countless companies and government agencies rely on.[26]

Early 2020s

Artificial Intelligence Tools and Technology

Companies such as OpenAI, Google, Meta, and Anthropic have emerged as dominant forces in AI development, raising concerns about competition, bias, and accountability in the rapidly evolving AI landscape.[27]

The Modern Digital Landscape and Hyperscalers

A few powerful entities—often termed hyperscalers[28] —dominate today's digital infrastructure and control vast portions of the internet's "logical layer" (the software and services that make the internet usable). While this concentration offers undeniable benefits such as efficiency, cost savings, and interoperability, it also creates societal risks that the U.S. government must address.

To better understand these societal risks, it is important to recognize how hyperscalers underpin not just data storage but also the software many of us rely on each and every day:

- Cloud storage providers offer the infrastructure for organizations to store and retrieve data;
- Cloud-based software solutions like productivity tools, communication platforms, and other Software as a Service (SaaS) offerings deliver the applications we use every day; and
- Even though SaaS providers deliver their services, most still rely on hyperscalers like AWS, Microsoft Azure, and Google Cloud Platform to host and operate their software.

This reliance makes the entire ecosystem heavily dependent on a few hyperscalers. The more SaaS providers build their services on hyperscaler platforms, the more concentrated—and vulnerable—the system becomes. A disruption at one hyperscaler could cascade across multiple SaaS providers, affecting millions of users and critical services. In other words, even the software solutions we think of as independent ultimately rest on the hyperscalers, tying the resilience of the digital ecosystem to just a few players.

This reliance is by design:

- Hyperscalers actively encourage SaaS companies to use their platforms because it increases their overall utilization, solidifies market dominance, and reinforces the economies of scale that underpin their operations; and
- This dependence has created a precarious ecosystem where the resilience of critical infrastructure is directly tied to the stability of a handful of hyperscalers.

Consolidation has introduced significant single points of failure, leaving essential services vulnerable to cyberattacks, software vulnerabilities, and operational errors. As more aspects of daily life—from health records to financial transactions—increasingly rely on digital infrastructure, the stakes of these vulnerabilities increase.

This centralization extends across key domains of critical infrastructure:

- Microsoft products account for nearly 85% of the market share in the U.S. government's productivity software;[29]
- Amazon, Microsoft, and Google control over two-thirds of the cloud services market; and[30]
- The cybersecurity sector reflects a similar trend, with Microsoft and CrowdStrike owning nearly 50% of the market for endpoint security products.[31]

This degree of consolidation poses cascading risks. A single vulnerability—whether through supply chain attacks[32] like the SolarWinds breach or exploitation of zero-day vulnerabilities—can disrupt operations across entire industries, endangering national security, public health, and economic stability. For example, a systemic failure in a hyperscaler's platform could simultaneously impact SaaS providers, cloud storage clients, and the customers who depend on those services, creating widespread and compounding disruption.

The digital world has implicated nearly every aspect of modern life, and the consolidation of its foundational infrastructure demands urgent attention. While the efficiencies offered by hyperscalers and SaaS providers have driven remarkable innovation, that consolidation has simultaneously created an ecosystem vulnerable to failure on a scale that is difficult to predict or fully mitigate.

Digital Consolidation as a Risk to Our Digital World and Modern Way of Life

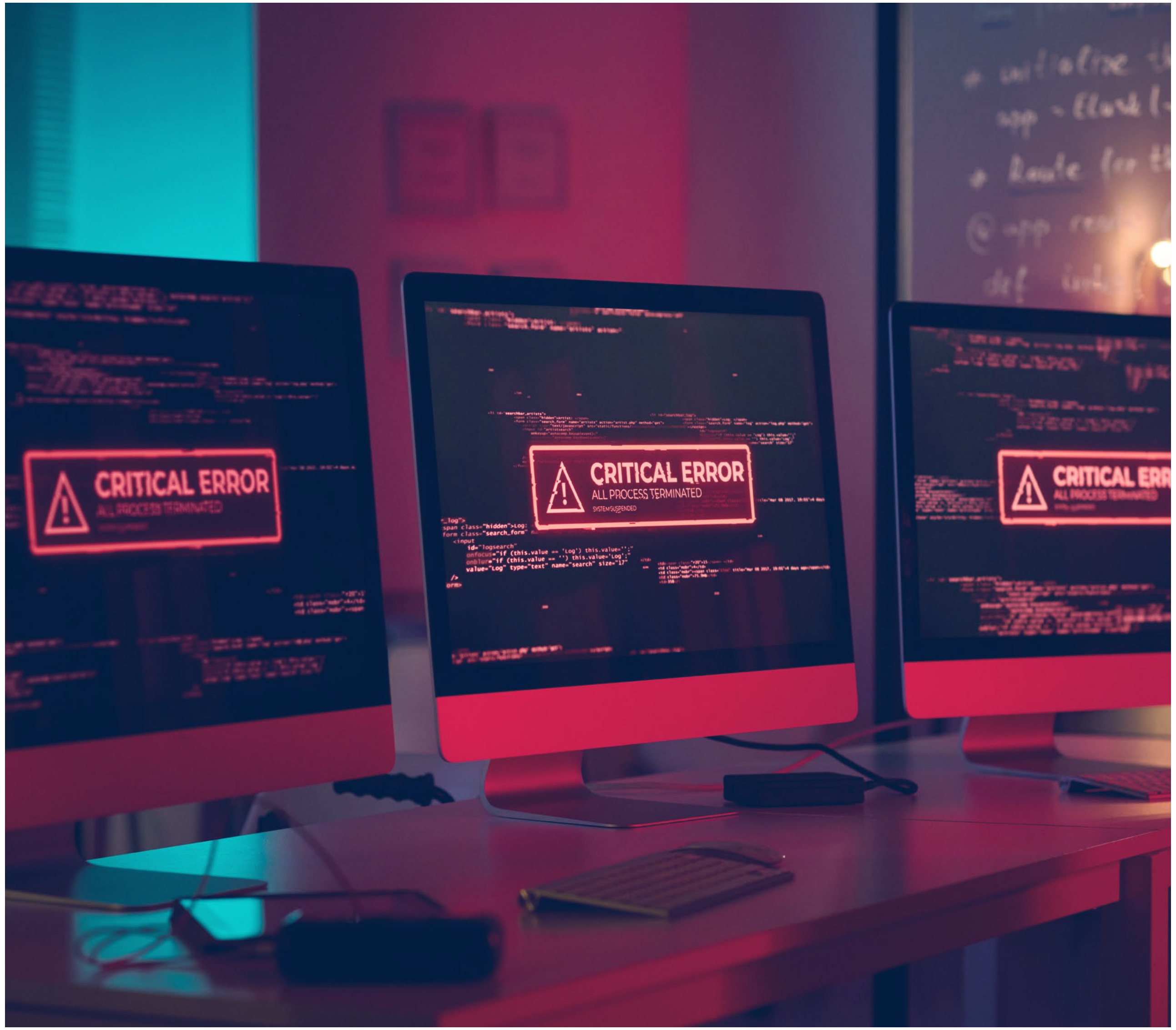
The physical and digital realms are inextricably linked. A disruption in one can quickly cascade into the other, compounding the risks in an increasingly interconnected world. By concentrating so much of our digital and physical infrastructure within a small number of entities, society has created a precarious ecosystem. This consolidation makes it easier for malicious actors to exploit single vulnerabilities, knowing that a breach in one system can compromise vast portions of our digital landscape.

Consolidated digital companies are often prime targets for cyberattacks due to their vast repositories of sensitive data and the potential impact of disrupting their operations. The more data a company consolidates, the more attractive it becomes to cybercriminals seeking to exploit vulnerabilities for financial gain, espionage, or reputational damage.

Examples Include:

- Yahoo experienced one of the most significant data breaches in history between 2013 and 2016, where over 3 billion user accounts were compromised by Russian hackers who exploited backdoors and stolen backups;[33]
- LinkedIn suffered a significant breach in 2021 when hackers scraped data from 700 million users, exploiting API vulnerabilities to access personal information;[34] and
- The 2021 Microsoft Exchange Server attack, which affected over 30,000 U.S. companies by exploiting zero-day vulnerabilities, demonstrated how critical infrastructure can be targeted on a large scale.[35]

These incidents underscore the heightened risk faced by consolidated digital entities. The number of users affected by these breaches are larger than most nation-states.



CyberRisk Alliance Study Captures Attitudes Toward Tech Consolidation

In October and November 2024, ICIT partnered with CyberRisk Alliance (CRA) to create The ICIT 2024 Digital Consolidation Study. It explores trends, challenges, and benefits associated with consolidating IT systems and cybersecurity tools and is based on insights from a survey of 302 IT, cybersecurity, and business executives recruited from the CRA audience, which includes readers of SC Media and CISOs from CRA's CyberRisk Collaborative membership.

The study shows that while some organizations are increasingly consolidating their IT systems and cybersecurity tools - In hopes of enhancing efficiency and compatibility and driven largely by cloud modernization efforts – they also understand and worry about the significant security challenges identified earlier in this report.

Other respondents are more reluctant to consolidate because, along with lower costs and customization, they see diversity of systems as something that is more difficult to attain.

The survey illustrates that, while some do see benefits in consolidation, most companies understand the increased cybersecurity risks that come with fewer and bigger platforms.

KEY FINDINGS

1. **Trends in Consolidation**
   a. A significant majority of organizations have moderately or highly consolidated IT systems (95%) and cybersecurity tools (93%).
   b. Cloud modernization is driving consolidation efforts, with many organizations emphasizing efficiency and compatibility.
2. **Benefits of Consolidation**
   a. IT consolidation leads to improved cybersecurity (55%), streamlined operations (46%), and cost savings (41%).
   b. Cybersecurity consolidation enhances detection and response efficiency (45%), reduces costs (41%), and improves tool compatibility (36%).
3. **Challenges and Drawbacks**
   a. Concerns about over-consolidation include heightened security risks (54% for cybersecurity, 52% for IT), vendor lock-in, and potential single points of failure.
   b. Non-consolidators cite higher costs, lack of standardization, and limited visibility as challenges, despite benefits like specialization and resilience.
4. **Cybersecurity Breach Trends**
   a. One in four respondents experienced a cybersecurity breach in the past year, underscoring ongoing vulnerabilities.
5. **Strategic Considerations**
   a. Respondents emphasize the need for regular risk assessments, diversified vendors, and AI-driven automation to mitigate risks while retaining consolidation benefits.
   b. Nearly two-thirds advocate for public policy to address vulnerabilities introduced by consolidation.

SURVEY DEMOGRAPHICS

Participants

IT professionals (61%), cybersecurity practitioners (23%), and business executives (16%), with director-level or higher roles.

Industries

High-tech (22%), manufacturing (19%), and business services (13%) were the most represented sectors.

Organization Size

90% of respondents work in midsize (47%) or large (43%) organizations.

America Must Ensure Resilience Against Digital Disaster and Societal Risk

The digital world reflects two competing models: the open and private internet championed by the United States and fellow democracies and the state-controlled, monitored systems of authoritarian regimes like China[36] and Russia.[37] The democratic model grants broad access and privacy protections, ensuring freedom of expression and innovation. However, this openness also introduces systemic vulnerabilities. Greater access means greater opportunities for malicious actors to exploit weaknesses, making the democratic internet more susceptible to disruption than its tightly controlled, state-monitored counterparts.

While this increased vulnerability poses a cybersecurity challenge, the open internet must endure. Its broad access and seamless connectivity support modern economies, drive innovation and reflect the democratic values America upholds worldwide. Ensuring its resilience—by addressing digital consolidation, enhancing redundancy, and building a distributed infrastructure—demonstrates that an open internet can remain both robust and secure, providing a stark alternative to authoritarian models.

The 4-Rs of Digital Resilience

RESOURCING

- Market forces alone have failed to drive the investments needed to mitigate the societal risk created by digital consolidation.
- The U.S. government must, therefore, make targeted and modest investments to facilitate such resilience.

RECOVERY

- Preparing for digital disasters caused or exacerbated by consolidation requires a paradigm shift in planning.
- Just as we prepare for physical disasters by establishing comprehensive recovery plans to restore critical systems, infrastructure, and public confidence following a significant disruption, we must similarly prepare for digital disasters.

REHEARSING

- Recovery from a large-scale digital disaster will require cooperation between the public and private sectors at an unprecedented speed and scale.
- To ensure preparedness, we must rigorously test recovery plans through collaborative exercises involving government and industry.
- These rehearsals should simulate real-world scenarios, focusing on coordinating efforts, allocating resources, and restoring critical systems efficiently.
- Such testing is essential to identify gaps and strengthen the cooperative frameworks necessary to mitigate the risks associated with digital consolidation.

RESPONSE

- Ambiguity in cyberspace emboldens malicious nation-state and criminal actors.
- To deter the exploitation of digital consolidation, the U.S. must articulate and enforce clear response policies, making it evident that any successful or attempted attack on private-sector consolidators will trigger a decisive response from the U.S. government.

Four Pillars of Resilience

Resourcing, Recovering, Rehearsing, and Responding

Resilience as a framing concept extends beyond a defensive strategy to a proactive framework to mitigate risks and ensures national stability. This report outlines a resilience framework that is based on four pillars: Resourcing, Recovery, Rehearsal, and Response. Together, these four pillars protect the digital ecosystem, deter adversaries, and ensure the United States is prepared for the challenges of an uncertain digital future.

Pillar 1: Resourcing—Investing in Resilience

Pillar 1: Resourcing—Investing in Resilience

Resourcing is the foundation of resilience, fostering diversity in our digital ecosystems. When we invest in multiple companies performing similar functions in the digital environment that can work collaboratively, we ensure redundancies and render failures in our essential processes less likely to be realized.

The urgency of resourcing resilience is—and has been—clear. Rapid advancements in the Internet of Things (IoT) and artificial intelligence (AI) have dramatically increased the complexity of our digital infrastructure, expanding vulnerabilities and raising the likelihood of "black swan" events—unforeseen crises with cascading effects.

Resilience can only be achieved with strong public-sector leadership. The private sector alone is unable to overcome market dynamics. The U.S. government must fund research, foster innovation, and incentivize public-private collaboration to address vulnerabilities. Absent strategic investment, the risks posed by digital consolidation will remain unacceptably high.

Federal resources can accelerate efforts to harden digital infrastructure. Investments should focus on fostering technological diversity, enabling interoperability, and developing advanced recovery systems. Strategic funding will mitigate risks and catalyze innovation, ensuring that systems are more adaptable and better prepared for emerging threats. China's aggressive pursuit of digital dominance—through both state-sponsored cyber operations and investment in global digital infrastructure—further amplifies the systemic risks posed by consolidation. U.S. investments must therefore prioritize diversifying digital infrastructure and emphasize the testing and validation of resilience towards normalization across the digital infrastructure

The benefits of resourcing resilience extend to all stakeholders. Technology companies gain stability and reputational benefits, the government ensures the continuity of critical services, and the American people are protected from cascading intrusions. Globally, a resilient U.S. digital infrastructure serves as a model for democratic societies, underscoring the strength of an open and secure internet. But building resilience comes at a cost. However, that cost pales in comparison to the potential consequences of inaction.

1.1 Mandate and Fund Interoperability and Recovery Standards

Congress should enact legislation mandating and assisting in funding digital interoperability and recovery standards. The legislation should direct the National Institute of Standards and Technology (NIST) to recommend systems and technologies to be designated as critical digital infrastructure and develop interoperability and recovery standards for such critical digital infrastructure to ensure redundancy in systems. While NIST will ensure the technical feasibility of such standards in its development process, Congress must ensure such standards, once set, are contractually allowable, i.e., vendor licensing agreements cannot prevent interoperability and recovery standards from being applied. The Cybersecurity and Infrastructure Security Agency (CISA) should enforce these standards. Congress should set a no later than date of two years from the enactment of the statute to the enforcement of the standards by the Sector Risk Management Agencies (SRMAs).

NIST's interoperability and recovery standards must prioritize seamless integration across platforms and between systems to enable continuity of operations during disruptions. This approach aligns with NIST's role in developing cybersecurity standards and best practices.[38]

To support adoption, Congress should establish and sufficiently fund a Cybersecurity Assurance Fund (CAF) to catalyze public-private innovation, prioritizing investments that bolster national security and reduce reliance on foreign technology. The CAF could be modeled after existing programs such as the imperfect but successful State and Local Cybersecurity Grant Program (SLCGP),[39] which has allocated $1 billion to help state and local governments strengthen their security infrastructure.[40]

CISA should be empowered to audit compliance and impose penalties for noncompliance, ensuring adherence. CISA's role in this capacity is already established, as demonstrated by their issuance of Binding Operational Directive (BOD) 23-01,[41] which directs federal civilian agencies to better account for what resides on their networks. By offering financial support, the government can effectively bridge the gap between current technological limitations and future resilience requirements.

Federal procurement policies and practices can serve as a powerful catalyst for widespread adoption, mandating that contractors managing critical systems meet stringent interoperability benchmarks. This approach is consistent with existing federal initiatives, such as the Technology Modernization Fund (TMF),[42] which supports federal agencies in accelerating IT modernization projects to enhance cybersecurity and secure sensitive Government systems. Contractors managing critical systems must meet interoperability benchmarks, creating market incentives for broader adoption. This approach ensures a cohesive and resilient digital ecosystem while reducing the risks posed by reliance on a few dominant providers.

Creating market-driven incentives and a structured regulatory framework will foster a more cohesive and adaptable digital ecosystem. The strategy reduces systemic risks associated with over-reliance on a limited number of technology providers while promoting innovation, collaboration, and national technological resilience. This comprehensive approach aligns with ongoing efforts across various federal agencies, including the Department of Defense's initiatives to modernize IT[43] and the Department of Energy's plans to enhance its Radiological Emergency Data for Decision-making Portal (R2DP).[44]

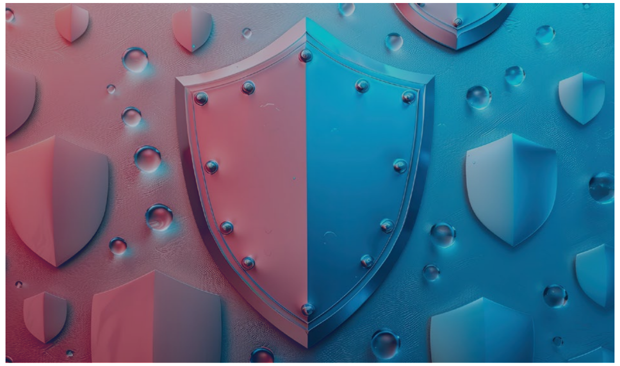
1.2 Enact a Cyber Insurance Relief Act

Congress should enact a Cyber Insurance Relief Act modeled on the Terrorism Risk Insurance Act (TRIA). This act should focus on mitigating the financial fallout of major cyber incidents or digital disasters. This legislation would adopt the approach of pooling risk while modernizing for the unique challenges of cyber events, including cascading failures across digital supply chains. After catastrophic cyber events, it would provide a federal backstop to ensure financial stability for businesses and critical infrastructure operators. A large-scale digital disaster seems increasingly likely, with determined and capable adversaries seeking to exploit the societal risk inherent in consolidated U.S. digital infrastructure.[45]

The TRIA has proven effective since its inception in 2002. It was designed to address the unavailability and high costs of terrorism insurance following the September 11 attacks, which could have severely hampered economic activity. By establishing a similar framework for cyber incidents, Congress can help stabilize the insurance market and encourage broader coverage for cyber risks that are increasingly recognized as significant threats to national security and economic stability.

The act should define triggering events, such as state-sponsored cyberattacks causing widespread disruption, and designate the Secretary of Homeland Security or the Director of CISA as certifying authorities. Including tax incentives and risk-sharing mechanisms would further encourage insurers to expand cyber coverage while ensuring that claims are processed swiftly to minimize operational downtime. As noted by industry experts, providing a federal backstop would enhance certainty in underwriting cyber risks, which is crucial given the current market's hesitance to cover such exposures adequately.[46]

A robust cyber insurance framework strengthens U.S. economic competitiveness by protecting critical industries and reassuring international partners of the nation's digital resilience. To achieve this aim, Congress should require insured entities to meet minimum cybersecurity standards, incentivizing resilience and reducing overall risk exposure. Aligning this effort with the 2027 TRIA reauthorization presents a strategic opportunity to conform cyber insurance reforms within existing risk frameworks, ensuring seamless integration and bipartisan support. The reauthorization process provides an opportunity to address emerging risks like cyber threats within existing frameworks, ensuring businesses remain resilient against traditional and modern threats. Given the societal risks posed by cyberattacks on the nation's concentrated digital infrastructure, a Cyber Insurance Relief Act could be instrumental in mitigating economic disruptions and enhancing the resilience of critical systems and actors.



1.3 Establish a Commission to Conduct a Review of Current Executive Branch Roles and Responsibilities for the Digital World

Congress should enact legislation establishing a bipartisan executive branch commission to review U.S. government agencies' current roles and responsibilities for the digital world. This Commission should examine and report back to Congress on how the U.S. government currently handles security and sustainability for the digital world, detailing current roles and responsibilities and explaining similarities to and distinctions from roles and responsibilities for the physical world. The purpose of this commission would be to resource Congress with an understanding of how the executive branch has formally and informally organized and functioned with the creation and growing centrality of the digital world. This role could be encompassed as part of the mandate undertaken by the newly created Department of Governmental Efficiency (DOGE). Its objective is to set forth the current state of affairs compared against the backdrop of the future ideal state and set forth the steps required to realize that objective.

1.4 Incentivize Public-Private Research and Development Targeting Near-Term Resilience Technologies and System Designs

Congress should enact legislation encouraging the near-term development of technologies and system designs to mitigate risks linked to digital consolidation by incentivizing robust public and private research and development. While the ultimate goal is to develop systems that are secure by design, the extensive presence of legacy systems and accumulated technical debt make this a protracted process.[47] Concurrently, adversaries, particularly state-sponsored actors from China,[48] are intensifying cyberattacks on our critical infrastructure for potential disruptive purposes. This confluence of factors creates a pressing need to expedite the implementation of robust near-term resilience technologies and systems to preserve our digital world. Immediate investments are needed to enhance the nation's technical capacity to respond to and recover from digital disruptions caused by cyberattacks targeting consolidated digital infrastructure or widespread digital disasters.

To achieve this, Congress should create initiatives that address systemic vulnerabilities without exacerbating consolidation risks, i.e., promote system and technology diversification. Programs like the Department of Energy's Innovation Network for Fusion Energy (INFUSE), which pairs private companies with National Laboratories to tackle fusion energy challenges, provide a proven model for such partnerships.[49] A similar approach could focus on critical areas such as quantum-safe cryptography, AI-driven threat detection, and next-generation recovery mechanisms. These investments will ensure that resilient technologies evolve with emerging threats and the rapid pace of technological change.

The history of successful public-private collaborations demonstrates the potential to drive innovation while safeguarding national security. By fostering partnerships that align cutting-edge research with actionable resilience measures, Congress can address the vulnerabilities inherent in today's highly consolidated digital ecosystem, protecting the nation's economic and security interests.

Pillar 2: Recovery Planning—Minimizing the Impact of Disruptions

Developing robust recovery plans for large-scale digital disruptions is essential to national resilience. In the physical world, the United States invests heavily in disaster response systems to restore order after natural catastrophes or crises. Similarly, in the digital world, recovery planning ensures that disruptions—whether caused by cyberattacks, technological failures, or natural disasters—are contained and essential services are swiftly restored. This capability minimizes downtime, mitigates cascading impacts, and prevents digital disruptions from escalating into broader societal crises.

Recovery is more than regaining functionality; it is a demonstration of national strength and an anchor of public trust. A well-executed recovery process reassures citizens of the nation's ability to endure and recover from adversity while signaling preparedness and resilience, deterring adversaries.

To achieve this, recovery efforts must be designed to address the systemic risks posed by digital consolidation. Clear benchmarks are needed to define success, and public-facing services should be prioritized to maintain continuity in critical functions. Public-private partnerships are vital to this effort, harmonizing resources and expertise from government and industry to build comprehensive recovery frameworks. By modernizing recovery practices and emphasizing collaboration, the U.S. can ensure it is prepared to respond to the challenges of a highly interconnected and consolidated digital world.

2.1 Establish Recovery Time Objectives Across Federal Systems

Congress should enact legislation that directs the Office of Management and Budget, in cooperation with the Chief Information Security Officer (CISO) Council, to mandate Recovery Time Objectives (RTOs) for mission-critical federal systems to ensure rapid restoration of essential services following a digital disruption. OMB should work with ONCD to ensure consistency in Federal RTOs with regulatory harmonization efforts and prioritize services like healthcare, financial systems, and disaster response, ensuring continuity during crises. This aligns with Maximum Tolerable Downtime (MTD) and RTOs as outlined in the Defense Contract Management Agency's continuity planning procedures.[50]

RTOs should be enforced through regular audits, interagency coordination, and progress reports to Congress. These benchmarks must address each sector's unique dependencies while fostering a unified national approach to recovery.

2.2 Modernize Procurement Practices to Enhance Resilience

The Office of Management and Budget should update federal procurement policies to prioritize vendor diversity, security performance, and recovery capabilities. These updates must prevent over-consolidation by encouraging diversified solutions that enhance service continuity and ensure adherence to interoperability and recovery standards.

Building on the framework established in *Recommendation 1.1 Mandate and Fund Interoperability and Recovery Standards*, procurement rules should explicitly require contractors managing critical systems to adhere to the interoperability benchmarks set by NIST. These standards must enable seamless integration across platforms and ensure recovery mechanisms, such as failover capabilities and adherence to RTOs, are technically feasible and contractually allowable. Vendor licensing agreements and practices[51] must not inhibit compliance with these standards, and CISA should audit and enforce adherence. Federal procurement practices must also account for the risks posed by vendors maintaining research, development, or manufacturing operations in countries of concern, particularly China, whose digital, economic, and security policies challenge U.S. security and values.

By modernizing procurement practices, the federal government can leverage its purchasing power to embed resilience as a cornerstone of digital infrastructure. This approach mitigates risks associated with over-consolidation and ensures the United States can withstand and recover from disruptions in an interconnected digital world.

2.3 Build a National Recovery Dashboard

CISA should create a centralized National Recovery Dashboard to monitor recovery readiness across sectors. This tool should track compliance with RTO benchmarks, highlight vulnerabilities, and provide actionable insights to guide response and recovery efforts.

The dashboard must standardize data collection and reporting across federal, state, and private-sector entities, ensuring transparency and accountability in recovery readiness.

2.4 Strengthen Public-Private Recovery Collaboration with Cross-Sector and Sector-Specific Continuity Frameworks

CISA should facilitate partnerships with private-sector stakeholders to harmonize recovery protocols and ensure consistency across industries. Shared recovery playbooks and joint planning sessions should address sector-specific risks and reduce confusion during crises, becoming a routine part of daily engagement.

Recovery drills, incorporating public and private participants, should regularly test these protocols to build trust and refine collaborative responses. CISA must actively engage the private sector to identify and mitigate risks from cyber threat actors, especially those targeting consolidated digital actors, systems, or capabilities, leveraging industry insights to fortify collective resilience against state-sponsored campaigns.

2.5 Enact Legislation to Create a Continuity-of-Services Framework

Congress should enact legislation directing ONCD to coordinate with federal agencies and private-sector leaders to create continuity-of-service frameworks tailored to critical sectors. These frameworks should define essential functions, prioritize their availability during crises, and establish protocols for rapid recovery. Recovery frameworks must explicitly consider scenarios involving coordinated attacks by advanced threat actors, ensuring that public and private entities are prepared for the unique challenges posed by these sophisticated adversaries.

Continuity frameworks should also include backup service provisions and redundancies for critical infrastructure, ensuring disruptions do not incapacitate essential systems.

Recovery is the linchpin of resilience. By establishing clear benchmarks, modernizing procurement, and fostering public-private collaboration, the United States is able to ensure its digital infrastructure can withstand and rebound from even the most severe disruptions. A strong recovery strategy is not just a safeguard for the digital world—it is a commitment to protecting the essential systems and services that sustain our way of life.

Pillar 3: Rehearsal—Preparing for Disruptions

Preparation enables resilience. In the physical world, the United States relies on disaster drills, emergency response rehearsals, and war games to save lives and safeguard infrastructure. Similarly, the digital world demands a robust and iterative approach to preparedness as cyber disruptions—whether from nation-state adversaries, internal system failures, or natural disasters—are not a question of "if" but "when" and "how often."

Frequent, scenario-based cyber rehearsals expose vulnerabilities, refine recovery protocols, and build stakeholder confidence across public and private sectors. These exercises ensure that participants are prepared to act decisively and collaboratively during crises. Rehearsals are not just about testing defenses; they help identify systemic weaknesses, foster trust, and strengthen partnerships across the digital ecosystem. By institutionalizing these exercises, the United States can create a fortified posture against adversaries and reduce the risk of cascading failures in critical infrastructure systems.

Rehearsals also send a clear message of readiness to adversaries, deterring exploitation. Exercises must address evolving nation-state tactics and sector interdependencies while ensuring comprehensive participation from state, local, tribal, and territorial (SLTT) entities and private-sector partners. This coordinated, whole-of-nation effort ensures national resilience and readiness for the inevitable.

3.1 Institutionalize National Cyber Rehearsals

Congress should enact legislation that mandates quarterly and annual cyber exercises to stress-test recovery protocols, cross-sector coordination, and failover mechanisms. ONCD should create a formal National Cyber Exercise Calendar, integrating federal agencies, private-sector stakeholders, and SLTT partners. Federal funding should support SLTT partners' participation in these exercises, ensuring their preparedness for attacks on localized systems like water utilities, healthcare networks, and regional power grids. Strengthened SLTT participation builds layered national defenses, enhancing resilience against regional vulnerabilities.

Quarterly exercises should focus on sector-specific vulnerabilities using scenarios informed by real-world intelligence on adversarial tactics. Critical sectors such as energy, healthcare, and finance should regularly rehearse incident response protocols to ensure readiness. Annual exercises must unite these sectors to test a unified national response to a complex, multi-vector cyberattack scenario.

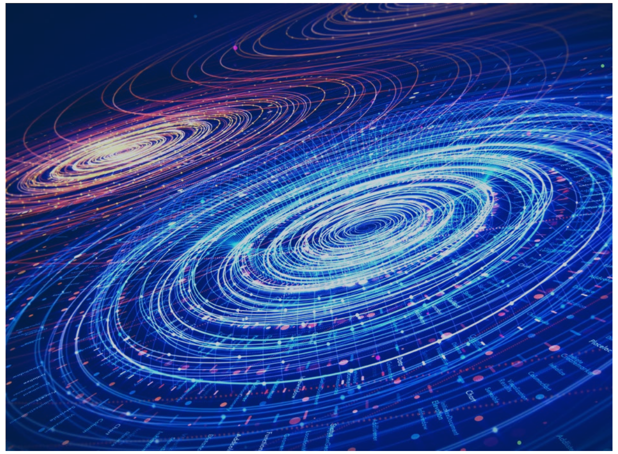
3.2 Address Nation-State Threat Scenarios in Exercises

Rehearsals must simulate the sophisticated tactics employed by adversaries like China, which leverage multi-phase attacks to disrupt entire networks. Modular exercises should mirror these threats, using downgraded intelligence-driven scenarios to replicate advanced techniques such as economic destabilization through cyber intrusions in financial systems. Cyber rehearsals must simulate advanced tactics Chinese threat actors use, such as supply chain compromises and multi-phase intrusions targeting critical infrastructure sectors.

3.3 Ensure Comprehensive Vendor and Private-Sector Participation

CISA should require major technology vendors and critical infrastructure operators to engage actively in cyber rehearsals. These exercises must evaluate their ability to recover from systemic failures, maintain operational continuity, and coordinate with public-sector partners. Vendor involvement should be formalized through public-private agreements, ensuring accountability and alignment with national resilience priorities.

These exercises will help identify and mitigate vulnerabilities in highly integrated digital ecosystems by testing large-scale failures in consolidated systems.



3.4 Implement Immediate Feedback Loops

ONCD should establish mechanisms to capture lessons learned from exercises and produce actionable recommendations within 30 days. Immediate post-exercise feedback sessions should provide real-time insights to government agencies, SLTT partners, and private-sector stakeholders to address identified vulnerabilities promptly.

Gap analyses must follow each exercise, outlining the areas where defenses are most vulnerable to nation-state threats. These analyses should guide resource allocation and policy development, ensuring continuous improvement and rapid adaptation to emerging risks. Budgetary allocations and statutory authorities must be made available to respond quickly as gaps are identified.

3.5 Develop a National Cyber Readiness Framework

Congress should enact legislation that directs ONCD and CISA to create a centralized National Cyber Readiness Framework. This framework will consolidate findings from rehearsals, track readiness metrics across sectors, and highlight vulnerabilities for prioritization. By integrating rehearsal outcomes into a national readiness framework, this tool will ensure transparency, accountability, and actionable progress.

3.6 Publish an Annual Cyber Resilience Report for Congress

An Annual Cyber Resilience Report should consolidate lessons learned from quarterly and annual exercises, evaluate national preparedness, and recommend targeted legislative and regulatory actions. Public-facing versions of the report should encourage private-sector improvements and broader participation in national resilience efforts. This requirement ought to be assigned to ONCD to implement.

Pillar 4: Response—Deterring Cyberattacks on Digital Consolidation

Resilience is incomplete without deterrence. While the first three pillars ensure the United States can endure disruptions, Pillar Four ensures that adversaries understand the costs of conducting a cyber-attack on the United States, targeting digital consolidation for disruption. A robust response framework should outline clear thresholds for action and enforce decisive consequences for those threatening the nation's consolidated digital infrastructure.[52]

Deterring cyberattacks on consolidated digital infrastructure requires a tailored approach. These attacks threaten not only the systems themselves but also the societal stability that relies on their uninterrupted operation. The challenge is heightened by the unique nature of the digital world, where much of the infrastructure is owned by private-sector entities, and the norms of international law are still evolving. While developing red lines for cyber deterrence is complex, establishing them is essential to protecting our digital world. The following focused recommendations assign clear roles to Congress, the Executive Branch, or both to implement actionable solutions.

4.1 Establish Clear Red Lines for Attacks Targeting Digital Consolidation

Congress and the Executive Branch should jointly define thresholds for U.S. responses to cyberattacks targeting consolidated infrastructure. These red lines must address attacks on actors, systems, and technologies essential to our economy, security, and modern way of life, e.g., hyperscalers, core SaaS providers, and critical AI systems. Congress should oversee and codify these thresholds to ensure clarity and consistency, while the Executive Branch implements them through executive orders and interagency coordination. Articulating such red lines will affirm the importance of the digital domain as a cornerstone of national resilience and a critical component of modern society that must be safeguarded.[53]

4.2 Develop Advanced Technical Attribution Capabilities

Congress should allocate targeted funding to the National Security Agency (NSA), Federal Bureau of Investigation (FBI), and the CISA to develop advanced attribution technologies specifically focused on threats exploiting digital consolidation. These capabilities should prioritize identifying adversaries targeting hyperscalers, core SaaS providers, and other consolidated systems critical to national infrastructure. Attribution efforts must leverage emerging technologies, such as AI-driven anomaly detection and blockchain forensic tools, tailored to track and trace attacks within interconnected digital ecosystems.

4.2.1 Foster Public-Private and International Collaboration in Attribution

Accurate attribution cannot be achieved in isolation. The Executive Branch, particularly through CISA and the ONCD, should formalize mechanisms for integrating private-sector entities into the attribution process. Since private-sector systems are often the targets of these attacks, their active involvement is critical for providing technical insights, access to incident data, and operational context.

Congress should support this effort by legislating protections to ensure companies can safely share data without fear of legal or reputational repercussions. These partnerships must emphasize trust-building, ensuring that private companies see their role in attribution as a shared responsibility in defending national infrastructure. By incorporating private-sector expertise and fostering collaborative relationships, the United States can build a more cohesive and reliable attribution framework.

Furthermore, the United States will need allies for attribution—and the action that may follow. The Executive Branch, led by the Department of State, should strengthen international collaboration with allied nations and private-sector consolidators to enhance attribution capabilities. Initiatives should include intelligence sharing on attacks targeting concentrated digital infrastructure and coordinated efforts to develop shared attribution frameworks. By focusing on threats tied to digital consolidation, these measures will ensure that adversaries exploiting these systemic vulnerabilities are identified quickly and accurately, enabling timely and decisive responses.

4.3 Develop a Tailored Cyber Response Doctrine

The Executive Branch should articulate a doctrine integrating proportional and multi-domain responses to attacks targeting consolidated infrastructure. This doctrine should leverage the full range of diplomatic, informational, military, and economic capabilities, ensuring the U.S. can respond decisively to cyberattacks targeting digital consolidation. Borrowing from the principles in the Tallinn Manual, the doctrine should clarify the application of international law, such as defining what constitutes a "use of force" or "armed attack" in the digital world while accounting for the private-sector ownership of much of the targeted infrastructure.[54]

4.4 Strengthen the Role of the Private Sector

Given the private sector's ownership and control over most consolidated digital infrastructure, the U.S. must strengthen partnerships to enhance both deterrence and resilience. Congress should expand liability protections for companies that share threat intelligence or assist in cyber response efforts, ensuring they can operate without fear of legal repercussions. While the Cybersecurity Information Sharing Act (CISA) of 2015[55] provides important protections and a framework for voluntary information sharing between the private sector and the federal government, further enhancements are necessary to address the unique risks posed by attacks targeting consolidated digital systems.

Building on CISA's foundation, Congress should legislate additional measures to encourage active private-sector participation in response efforts, particularly during incidents that threaten national infrastructure. These partnerships must also define the roles of private entities in cyber incidents, ensuring clear guidance on how their efforts align with inherently governmental functions. By codifying these roles and responsibilities, the U.S. can reduce ambiguity, foster trust, and ensure a coordinated response that maximizes the collective capabilities of both public and private stakeholders.

4.5 Integrate Resilience into Deterrence

Congress should allocate funding to federal agencies such as CISA and U.S. Cyber Command to develop and implement national resilience strategies tailored to the risks of digital consolidation. Additionally, the Executive Branch should issue directives mandating that resilience planning be a core component of cybersecurity policies across federal agencies, emphasizing redundant systems, failover mechanisms, and recovery capabilities.

Resilience and deterrence are mutually reinforcing. Demonstrating the ability to rapidly recover from attacks targeting digital consolidation reduces adversaries' incentive to disrupt these systems. Investments in redundant systems, failover mechanisms, and advanced recovery capabilities must be prioritized, signaling to adversaries that any attack will fail to achieve its intended objectives.

Conclusion

Building Resilience in an Era of Digital Consolidation

The U.S. government faces an urgent mandate: to secure a digitally consolidated world that underpins the nation's economy, security, and daily life. The Four Rs—Resourcing, Recovery, Rehearsal, and Response—represent a comprehensive framework for building resilience and ensuring the digital domain can withstand and recover from the disruptions that adversaries are increasingly determined to inflict. These pillars are not abstract ideals but actionable steps that demand immediate attention and investment.

Resilience begins with strategic resource allocation, ensuring that digital systems are robust, interoperable, and adaptable to unforeseen challenges. It extends to meticulous recovery planning, enabling rapid restoration of critical systems after a disruption. Rehearsal cements these efforts, testing recovery protocols through coordinated public-private exercises that expose vulnerabilities and strengthen trust among stakeholders. Finally, response reinforces resilience by articulating clear deterrence policies that establish red lines and impose decisive consequences for cyberattacks targeting consolidated infrastructure.

The risks of inaction are clear. Consolidation has introduced efficiencies but also created systemic vulnerabilities that adversaries can exploit to cause widespread disruption. The time to act is now. By embracing this framework, Congress and the Executive Branch can fortify the nation's digital ecosystem, mitigate societal risks, and ensure the United States remains a global leader in the digital age.

This is not just a matter of safeguarding our digital world; it is about securing the trust, stability, and resilience that define our nation's strength. The digital world has transformed how we live, work, and engage with one another. Protecting it is no longer discretionary—it is mandatory for the future of American leadership and prosperity.

Appendices

Task Force Members

Marene Allison, *Retired Vice President and CISO at Johnson & Johnson*

Ms. Allison protected Johnson & Johnson information technology systems and business data worldwide. This included ensuring that the company's information security posture supported business growth objectives, protected public trust in the Johnson & Johnson brand, and met legal/regulatory requirements.

Prior to joining Johnson & Johnson, Ms. Allison was Chief Security Officer and Vice President for Medco, the largest pharmacy benefit manager in the United States. Ms. Allison was responsible for all aspects of the company's security, regulatory and compliance including, physical and logical security, executive protection as well as HIPPA, Payment Card Industry, Medicare and prescription fraud and IT controls.

Prior to that, Ms. Allison was with Avaya as head of Global Security where she worked on securing the World Cup network in Korea and Japan in 2002. Before joining Avaya, she was Vice President of Loss Prevention and Safety for the Great Atlantic and Pacific Tea Company. Before joining the corporate world, she served as a Special Agent in the FBI working on undercover drug operations in Newark, NJ, while also working on terrorist bombings in San Diego, CA. She developed and participated in the nuclear terrorism exercise, Compass Rose '88, the largest mock terrorism incident exercise by the federal government.

Ms. Allison has a Bachelor of Science degree from The United States Military Academy at West Point, in the first class to include women. She has served in the US Army in the Military Police, at Ft Hood, TX, Ft Chaffee, AR and Ft McClellan, AL. She has served on the Defense Advisory Committee on Women in the Services appointed by the Secretary of Defense and the Overseas Security Advisory Committee appointed by the Secretary of State. Marene is a founding member of West Point Women and currently serves on their Board of Directors. She is also on the Board of Directors for H-ISAC (Health Information Sharing and Analysis Center) and ASIS International.

Nicholas Andersen, *Chief Operating Officer at Invictus International Consulting*

Nick Andersen is the Chief Operating Officer (COO) for Invictus International Consulting – a recognized market leader in full-spectrum cyber solutions designed to ensure the security of our nation's global defense and critical infrastructure. Prior to his role at Invictus, Andersen served as the Public Sector Chief Information Security Officer (CISO) for Lumen Technologies, a telecommunications provider with approximately 450,000 route fiber miles and customers in more than 60 countries.

Andersen previously served as the Principal Deputy Assistant Secretary and performed the duties of the Assistant Secretary for Cybersecurity, Energy Security, and Emergency Response (CESER) at the U.S. Department of Energy. He was appointed to lead DOE's national effort to secure U.S. energy infrastructure against all hazards, reduce impacts from disruptive events, and assist industry with restoration activities. Before joining the Department of Energy, Nick served in the White House Office of Management and Budget (OMB) as the Federal Cybersecurity Lead and Senior Cybersecurity Advisor to the Federal Chief Information Officer, where he led the OMB Cyber Team and was responsible for government-wide cybersecurity policy development and compliance of shared federal security services.

Andersen was a senior executive and senior intelligence officer serving as the Chief Information Officer for Navy Intelligence and was the Chief of the Office of Intelligence, Surveillance, and Reconnaissance Systems and Technologies at the U.S. Coast Guard. He has served on active duty with the U.S. Marine Corps, managing intelligence mission systems in Iraq, Europe, and Africa. He has led cybersecurity and technology programs worldwide with several leading and emerging companies.

Andersen has earned a Bachelor of Science in Information Technology Management, a Master of Science in Information Security and Assurance, and more recently a Master of Science in Cybersecurity from Brown University, and an Executive Certificate in Public Policy from the Harvard Kennedy School. He has received awards from the U.S. Navy, U.S. Marine Corps, U.S. Coast Guard, and Intelligence Community.

Edna Conway, *CEO of EMC Advisors*

Edna Conway is CEO of EMC Advisors, providing board and advisory services to enterprises and governments globally on technology, security, risk management and supply chain resilience. She most recently served as Microsoft's chief security & risk officer for cloud infrastructure, ensuring the security and resilience of the Azure cloud infrastructure.

Previously, Conway served as Cisco's chief security officer, global value chain, a partner in an international private legal practice and assistant attorney general for the State of New Hampshire. She holds an AB from Barnard College, a law degree from the University of Virginia and additional credentials from MIT, Stanford, Carnegie Mellon and New York University. Conway is an advisor to capital investment organizations, has served on over a dozen boards and is an inductee into the ranks of Fortune's Most Powerful Women. She serves on the NYU Tandon School of Engineering Cyber Fellows Advisory Council as faculty for the Carnegie Mellon University CISO Program and the Institute for Applied Network Research. Conway is also a senior non-resident fellow at Carnegie Endowment for International Peace.

Brett Freedman (Task Force Co-Chair), *Founder and President of Canopy Consulting Group*

Brett Freedman is the Founder and President of Canopy Consulting Group, a strategic advisory firm, and served as the Chief of Staff for Assistant Attorney General Matthew G. Olsen of the National Security Division at the Department of Justice. Previously, Brett spent seven years working for the Senate Select Committee on Intelligence as both Minority Counsel for Senator Dianne Feinstein and as General Counsel for Chairman Mark Warner.

Previously, Mr. Freedman served worked as an attorney in Executive Branch roles in the National Counterterrorism Center of the Office of the Director of National Intelligence and at the National Security Agency's Office of General Counsel. In 2013, Brett was selected to serve as Counsel to the President's Review Group on Intelligence and Communications Technologies that stood up following the unauthorized disclosures by Edward Snowden.

Earlier in his career, Brett served as a Presidential Management Fellow for DHS in the Bureau of Customs and Border Protection and as an Advisor to Former Secretary Ridge in the Office of International Affairs. Brett's career in public service began after college when he was hired as a Legislative Assistant for Congressman Michael E. Capuano.

Brett received his Bachelor of Arts in International Relations from Boston University, a Master of Arts in Law and Diplomacy from the Fletcher School at Tufts University, and a Juris Doctor degree from Suffolk University Law School.

Ankur Sheth, *Senior Managing Director and Global Lead of the Technology and Cyber Risk Practice at Ankura*

Ankur Sheth is based in New York where he serves as Senior Managing Director and Global Lead of Ankura's Technology and Cyber-Risk Practice Ankur has been focused on cybersecurity for over 20 years across a variety of competencies and industries and continues to serve his clients in successfully mitigating potential cyber threats.

Ankur possesses an extensive knowledge of cybersecurity controls, processes, and technologies, and continues to assist clients with projects ranging from strategy to implementation. He has worked with clients across multiple industries ranging from financial services to healthcare and beyond to help them strategize, analyze, plan, architect, design, implement, and support cybersecurity related controls and systems. Ankur utilizes extensive education and experience along with his business and security knowledge to deploy leading practices across all security aspects within enterprises. Additionally, Ankur has worked with his multi-national clients at a global level across North and South America, Europe, Middle East, and Asia Pacific.

Ankur regularly works with risk and IT officers and executive and board members on the changing cybersecurity landscape and the best approaches for managing that ongoing risk in an effective and efficient manner. Ankur has helped build and develop cybersecurity programs at organizations that employ leading technologies and practices to enhance their overall security posture.

Cory Simpson (Task Force Co-Chair), *Chief Executive Officer of the Institute for Critical Infrastructure (ICIT) and Gray Space Strategies*

ICIT is a nonprofit, nonpartisan, 501(c)3 think tank with the mission of modernizing, securing, and making resilient critical infrastructure that provides for people's foundational needs. Gray Space Strategies is a professional services and strategic advisory firm based in Washington, D.C., that specializes in assisting clients in navigating the U.S. government and emerging technology markets, cybersecurity ecosystem, and national security spaces. Cory volunteers as a senior advisor to CSC 2.0, continuing the work of the U.S. Cyberspace Solarium Commission, and is on the Board of Directors for The Cyber Guild.

Cory previously worked as a managing director at Ankura and as an executive vice president at Resolute Strategic Services. Before entering the private sector, Cory served for over 20 years in the national security community. Today, he is recognized as one of the nation's leading experts on cybersecurity, public and foreign policy, emerging technologies and their markets, and the pressing need to align economic policy with national security.

Cory served on active duty in the Army Judge Advocate General's Corps from 2004 to 2016 and continues to serve in the Army Reserve as a legal advisor to the U.S. Army Cyber Command. Cory has spent most of his military career as a general counsel, a prosecutor, and a national security law advisor. His highly decorated service includes multiple combat tours, several leadership roles, and extensive trial and advocacy experience. He is a sought-after speaker and lecturer on cybersecurity, national security, technology policy, and foreign relations. He earned a Juris Doctorate from the West Virginia University College of Law; a Master of Laws, Military Law from The Judge Advocate General's Legal Center and School in Charlottesville, VA; and a BA in accounting with a minor in philosophy from Transylvania University.

Acknowledgments

The Task Force wishes to thank numerous people without whom the report would not have been possible. In particular, the Task Force would be remiss if it did not acknowledge its gratitude to Bianca Andre and Tanner Wilburn. Ms. Andre has a diverse background in legislative affairs, contributing to significant legislation such as the Broadband DATA Act. Mr. Wilburn is a J.D. candidate at the Indiana University Maurer School of Law and a Fellow at Indiana University's Center for Applied Cybersecurity Research.

About The Institute for Critical Infrastructure Technology

The Institute for Critical Infrastructure Technology (ICIT) is a nonprofit, nonpartisan, 501(c)3 think tank whose mission is modernizing, securing, and making resilient critical infrastructure that provides for people's foundational needs. ICIT takes no institutional positions on policy matters. Rather than advocate, ICIT is dedicated to being a resource for the organizations and communities that share our mission.

Founded in late 2014, the Institute's work has earned the trust and respect of the nation's most influential institutions and serves a diverse community of technology, policy, and business leaders. By applying a people-centric lens to critical infrastructure research and decision-making, our work ensures that modernization and security investments have both a lasting and a positive impact on society.

About CyberRisk Alliance

CyberRisk Alliance provides business intelligence that helps the cybersecurity ecosystem connect, share knowledge, accelerate careers, and make smarter and faster decisions. Through its trusted information brands, network of experts, and innovative events it provides cybersecurity professionals with actionable insights and act as a powerful extension of cybersecurity marketing teams. CyberRisk Alliance brands include SC Media, the Official Cybersecurity Summits, TechExpo Top Secret, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, Cybersecurity Collaborative, Security Weekly, ChannelE2E, MSSP Alert, and LaunchTech Communications.

Notes

[1] Heather Boushey & Helen Knudsen, The Importance of Competition for the American Economy. THE WHITE HOUSE COUNCIL OF ECON. ADVISERS (July 09, 2021), https://www.whitehouse.gov/cea/written-materials/2021/07/09/the-importance-of-competition-for-the-american-economy/.

[2] Societal risk refers to the likelihood and potential impact of events that can cause widespread harm to a significant portion of society, including its people, infrastructure, or social systems.

[3] *Consequence-Driven Cyber-Informed Engineering*, IDAHO NAT'L. LAB'Y., https://inl.gov/national-security/cce/ (last visited Dec. 3, 2024).

[4] Sadia Rahman, The Cable Ties to China's Digital Silk Road, THE LOWY INST. (Apr. 29, 2024), https://www.lowyinstitute.org/the-interpreter/cable-ties-china-s-digital-silk-road.

[5] Yanzhong Huang, *Tipped Power Balance: China's Peak and the U.S. Resilience*, COUNCIL ON FOREIGN REL. (Feb. 22, 2024). https://www.cfr.org/blog/tipped-power-balance-chinas-peak-and-us-resilience.

[6] In the first Trump Administration, see e.g., *Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, 82 Fed. Reg. 22391 (May 11, 2017); *Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed. Reg. 22689 (May 15, 2019); *Secure and Trusted Communications Networks Act*, Pub. L. No. 116-124, 134 Stat. 158 (2020) (codified at 47 U.S.C. §§ 1601–1609); *Executive Order 13942: Addressing the Threat Posed by TikTok*, 85 Fed. Reg. 48637 (Aug. 6, 2020); *Executive Order 13943: Addressing the Threat Posed by WeChat*, 85 Fed. Reg. 48641 (August 6, 2020). In the Biden Administration, see e.g., *Executive Order 14028: Improving the Nation's Cybersecurity*, 86 Fed. Reg. 26633 (May 12, 2021); Secure Equipment Act, Pub. L. No. 117-55, 135 Stat. 423 (Nov. 11, 2021) (codified at 47 U.S.C. § 1601); *Executive Order 14105: Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern*, 88 Fed. Reg. 54867 (Aug. 9, 2023); Elaine Kurtenbach, *US Expands List of Chinese Technology Companies Under Export Controls*, Associated Press (Dec. 3, 2024), https://apnews.com/article/china-us-technology-chips-sanctions-bis-8f8ab1ab49b5bb57e5a290a3937fa939.

[7] *Cyberspace*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/topic/cyberspace (last visited Nov. 19, 2024).

[8] *March 17, 1948: William Gibson, Father of Cyberspace,* WIRED (Mar. 16, 2009), https://www.wired.com/2009/03/march-17-1948-william-gibson-father-of-cyberspace-2/.

[9] *New York State Alerts New Yorkers of Temporary Electronic Benefits Transfer (EBT) Outage on Sunday, May 19, for System Updates EBT*, NEW YORK STATE OFF. OF TEMP. AND DISABILITY ASSISTANCE (May 15, 2024), https://otda.ny.gov/news/2024/2024-05-15.asp.

[10] *The Cyber-Nuclear Threat*, NUCLEAR THREAT INITIATIVE (Oct. 31, 2022), https://www.nti.org/analysis/articles/cyber/.

[11] Security experts have been discussing software monocultures for decades. See D.E. Geer, C.P. Pfleeger, B. Schneier, J.S. Quarterman, P. Metzger, R. Bace, & P. Gutmann, *Cyberinsecurity: The Cost of Monopoly*, COMPUT. & COMMC'NS INDUS. ASS'N (Sept. 24, 2003), https://ccianet.org/wp-content/uploads/2003/09/cyberinsecurity%20the%20cost%20of%20monopoly.pdf.

[12] *See* Andrew Welsch, *Osaic CEO Says Consolidation Efforts Are Nearing Completion*, BARRON'S ADVISOR (Sept. 20, 2024), https://www.barrons.com/advisor/articles/osaic-ceo-jamie-price-consolidation-eb904603. This is a recent example in the financial services sector, where Osaic has nearly completed consolidating its network of eight broker-dealers, transitioning over 11,000 financial advisors managing assets exceeding $700 billion onto a unified platform. *See also* Nick Huber, *Generative AI Turns Spotlight on Contract Management*, FINANCIAL TIMES (July 3, 2024), https://www.ft.com/content/1026fd13-d7f1-40de-a0d6-9e4843ac3d29. In the legal technology domain, the integration of generative AI has spurred mergers and partnerships among contract lifecycle management software providers. Companies like DocuSign have acquired AI-powered firms such as Lexion, while Icertis has partnered with Evisort, indicating a consolidation trend to offer comprehensive AI-enhanced solutions for legal tasks.

[13] "It is the part of a wise man to keep himself today for tomorrow, and not venture all his eggs in one basket." Miguel de Cervantes, *Don Quixote* (1605). The phrase, "Don't put all your eggs in one basket," is a metaphor that means avoid putting all your resources or effort into one thing, as you might lose everything if it fails. It is a foundational principle of risk management.

[14] According to the International Monetary Fund (IMF), the occurrence of cyberattacks has doubled since the onset of the COVID-19 pandemic, *Key Cyber Security Statistics for 2024*, SENTINELONE, https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/ (last visited Dec. 3, 2024). Additionally, the U.S. Government Accountability Office (GAO) reported that data breaches of personally identifiable information (PII) within the Department of Defense more than doubled since 2015. U.S. Gov't Accountability Off., *DOD Cybersecurity: Enhanced Attention Needed to Ensure Cyber Incidents Are Appropriately Reported and Shared*, GAO-23-105084, https://www.gao.gov/assets/gao-23-105084.pdf. *See also* Microsoft Digital Defense Report 2024, at 39, MICROSOFT, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024 (last visited Dec. 3, 2024).

[15] Evan Morgan, *Eroding Global Stability: The Cybersecurity Strategies Of China, Russia, North Korea, And Iran*, IRREGULAR WARFARE INITIATIVE (Aug. 1, 2024), https://irregularwarfare.org/articles/eroding-global-stability-the-cybersecurity-strategies-of-china-russia-north-korea-and-iran/.

[16] Cyber Safety Review Board, *Review of the Summer 2023 Microsoft Exchange Online Intrusion*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Mar. 20, 2024), https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf.

[17] *Preliminary Post Incident Review (PIR): Content Configuration Update Impacting the Falcon Sensor and the Windows Operating System (BSOD)*, CROWDSTRIKE (July 25, 2024), https://www.crowdstrike.com/en-us/blog/falcon-content-update-preliminary-post-incident-report/.

[18] Evan Gorelick & Bloomberg, *CrowdStrike Outage Will Cost Fortune 500 Companies $5.4 Billion in Damages*, FORTUNE (Aug. 3, 2024), https://fortune.com/2024/08/03/crowdstrike-outage-fortune-500-companies-5-4-billion-damages-uninsured-losses/.

[19] We deliberately constrained our scope to avoid exploring large-scale U.S. government-to-industry recommendations, such as designating Cloud Service Providers (CSPs) as critical infrastructure with an associated Sector Risk Management Agency (SRMA) or advocating for significant market regulatory changes like new antitrust laws. This limitation reflects the nature of this report and our focus on actionable, near-term measures to enhance resilience to the societal risks posed by digital consolidation within the next two to four years.

[20] Kevin Featherly, *ARPANET*, ENCYCLOPEDIA BRITANNICA (Nov. 7, 2024), https://www.britannica.com/topic/ARPANET.

21. Tom Wheeler, *Big Tech Won. Now What?*, BROOKINGS INST. (Oct. 16, 2023), https://www.brookings.edu/articles/big-tech-won-now-what/#:~:text=Tom%20Wheeler%20Visiting%20Fellow%20-%20Governance%20Studies%2C%20Center,relations%20and%20the%20creation%20of%20new%20regulatory%20structures.

22. See James W. Cortada, *Change and Continuity at IBM: Key Themes in Histories of IBM*, CAMBRIDGE UNIV. PRESS (Mar. 26, 2018), https://www.cambridge.org/core/journals/business-history-review/article/change-and-continuity-at-ibm-key-themes-in-histories-of-ibm/DADE64DDC8569B2F9046B4CF47DFA814.

23. *See* U.S. Dep't of Justice, Antitrust Div., *U.S. v. Microsoft: Proposed Findings of Fact*, https://www.justice.gov/atr/us-v-microsoft-proposed-findings-fact-0 (last visited Dec. 3, 2024).

24. *See* Lionel Sujay Vailshery, *Oracle – Statistics & Facts*, STATISTA (Sept. 27, 2024), https://www.statista.com/topics/2509/oracle

25. *See* Lauren Feiner, *Breaking Down the DOJ's Plan to End Google's Search Monopoly*, THE VERGE (Nov. 27, 2024), https://www.theverge.com/2024/11/27/24302415/doj-google-search-antitrust-remedies-chrome-android.

26. *See* Felix Richter, *Amazon Maintains Cloud Lead as Microsoft Edges Closer*, STATISTA (Nov. 1, 2024), https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers.

27. *See* Matt O'Brian, *FTC Opens Inquiry Into Big Tech's Partnerships with Leading AI Startups*, ASSOCIATED PRESS (Jan. 25, 2024), https://apnews.com/article/ftc-antitrust-inquiry-openai-chatgpt-microsoft-anthropic-google-amazon-67feef411ef311f0be543f546ef34b3d.

28. *See* Alex Torres, *Hyperscalers: From Data Centers to Cloud Marketplaces*, INVISORY (April 17, 2024), https://invisory.co/resources/blog/what-is-a-hyperscaler-history-from-data-centers-to-cloud-marketplaces.

29. As stated in the House Committee on Homeland Security's recent letter to Brad Smith, Vice Chair and President, Microsoft Corporation, "[i]t is imperative that Microsoft, which accounts for nearly 85 percent of the market share in the U.S. government's productivity software, be held to the same level of accountability as the rest of the U.S. government's trusted vendors." U.S. House Comm. on Homeland Sec., *Letter to Brad Smith, Vice Chair and President, Microsoft Corp.*, at 2 (May 9, 2024), https://homeland.house.gov/wp-content/uploads/2024/05/2024-05-09-CHS-to-Microsoft-Request-to-Testify.pdf (citing *New Study Shows Microsoft Holds 85% Market Share in U.S. Public Sector Productivity Software*, COMPUT. & COMMC'NS INDUS. ASS'N (Sept. 21, 2021), https://ccianet.org/news/2021/09/new-study-shows-microsoft-holds-85-market-share-in-u-s-public-sector-productivity-software/.).

30. Mark Haranas, *Cloud Market Share In Q2: Microsoft Drops, Google Gains, AWS Remains Leader*, CRN (Aug. 7, 2024), https://www.crn.com/news/cloud/2024/cloud-market-share-in-q2-microsoft-drops-google-gains-aws-remains-leader?page=1&itc=refresh.

31. Rob Lefferts, *Microsoft again ranked number one in modern endpoint security market share*, MICROSOFT SEC. BLOG (Aug. 21, 2024), https://www.microsoft.com/en-us/security/blog/2024/08/21/microsoft-again-ranked-number-one-in-modern-endpoint-security-market-share/.

32. Emma Zaballos, *Why Software Supply Chain Attacks Persist*, SC MEDIA (Oct. 24, 2024), https://www.scworld.com/perspective/why-software-supply-chain-attacks-persist.

33. Nicole Perlroth, *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, THE N.Y. TIMES (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.

34. Catalin Cimpanu, *Hackers Leak LinkedIn 700 Million Data Scrape*, THE RECORD (Sept. 21, 2021); https://therecord.media/hackers-leak-linkedin-700-million-data-scrape.

35. Ian Sherr, *Microsoft Exchange Attackers Strike More Than 30,000 US Organizations*, CNET (Mar. 5, 2021); https://www.cnet.com/news/privacy/microsoft-exchange-attackers-strike-more-than-30000-us-organizations/.

36. Rodion Ebbighausen, *Decoding China: Who will shape the internet of the future?*, DIGITAL WORLD (May 26, 2024), https://www.dw.com/en/decoding-china-who-will-shape-the-internet-of-the-future/a-69174770.

37. Gleb Stolyarov & Lucy Papachristou, *Russia to Spend Over Half a Billion Dollars to Bolster Internet Censorship System*, REUTERS (Sept. 10, 2024), https://www.reuters.com/world/europe/russia-spend-over-half-billion-dollars-bolster-internet-censorship-system-2024-09-10/.

38. *Biden-Harris Administration Announces First-ever Consortium Dedicated to AI Safety*, NAT'L INST. OF STANDARDS & TECH. (Feb. 8, 2024), https://www.nist.gov/news-events/news/2024/02/biden-harris-administration-announces-first-ever-consortium-dedicated-ai.

39. Investing in a New Vision for the Environment and Surface Transportation in America Act (INVEST in America Act), H.R. 3684, 117th Cong. (2021) (as received by the Senate), https://www.congress.gov/117/bills/hr3684/BILLS-117hr3684pcs.pdf.

40. *State and Local Cybersecurity Grant Program*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/cybergrants/slcgp (last visited Dec. 3, 2024).

41. *BOD 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Oct. 3, 2022), https://www.cisa.gov/news-events/directives/bod-23-01-improving-asset-visibility-and-vulnerability-detection-federal-networks.

42. *Technology Modernization Fund*. U.S. GEN. SERVICES ADMIN., https://www.gsa.gov/technology/government-it-initiatives/technology-modernization-fund (last visited Dec. 3, 2024).

43. *Digital Modernization Strategy (DMS): Related Enterprise Information Technology Initiatives*, U.S. DEPT. OF DEF., https://www.dote.osd.mil/Portals/97/pub/reports/FY2021/dod/2021dms.pdf?ver=TN5m6zeMc9hKhxQp7Z1opw%3D%3D (last visited Dec 3, 2024).

44. *Technology Modernization Fund Announces Investments in Nuclear Safety and AI Governance*. U.S. GEN. SERVICES ADMIN. (July 19, 2024), https://www.gsa.gov/about-us/newsroom/news-releases/technology-modernization-fund-announces-investments-in-nuclear-safety-and-ai-governance-07192024.

45. *Consequence-Driven Cyber-Informed Engineering, supra* note 3.

46. *A Public-Private Partnership Approach to Federal Cyber-Insurance Backstop*, BUS. EXECUTIVES FOR NAT'L SEC. (July 23, 2024), https://bens.org/a-public-private-partnership-approach-to-a-federal-cyber-insurance-backstop/.

47. Peter Danhieux, Strategic Secure-By-Design Initiatives: Best Practices for Meaningful Outcomes, FORBES (Nov, 19, 2024), https://www.forbes.com/councils/forbestechcouncil/2024/11/19/strategic-secure-by-design-initiatives-best-practices-for-meaningful-outcomes/.

48. Attacks on the US from China Increasing, CYBER SEC. INTELLIGENCE (Dec. 12, 2024), https://www.cybersecurityintelligence.com/blog/attacks-on-the-us-from-china-increasing-8102.html.

49. Oak Ridge National Laboratory, *What is INFUSE?*, U.S. DEPT. OF ENERGY, https://infuse.ornl.gov/what-is-infuse/ (last visited Dec. 3, 2024).

50. *DCMA MAN 3301-02: Continuity of Operations and Emergency Management*, DEF. CONTRACT MGMT. AGENCY (Sept. 7, 2018),.https://www.dcma.mil/Portals/31/Documents/Policy/DCMA_MAN_3301-02.pdf.

51. Renee Dudley, with research by Doris Burke, *Microsoft's "Free" Plan to Upgrade Government Cyber-security Was Designed to Box Out Competitors and Drive Profits, Insiders Say*, PROPUBLICA (Nov. 15, 2024), https://www.propublica.org/article/microsoft-white-house-offer-cybersecurity-biden-nadella.

52. Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Harvard Univ. Press 2020).

53. *See generally*, https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/isec_a_00266.pdf, for the importance of establishing clear red lines in cyber deterrence strategy and also aligns with the principle that creating a tailored response framework for significant cyber threats, particularly those targeting consolidated digital infrastructure, is essential for a robust national cybersecurity strategy. Microsoft, *supra* note 14, at 22. See generally, Joseph S. Nye Jr., Deterrence and Dissuasion in Cyberspace, 41 INT'L. SEC. 3, 44–71 (Winter 2016/17), https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/isec_a_00266.pdf, for the importance of establishing clear red lines in cyber deterrence strategy and alignment with the principle that creating a tailored response framework for significant cyber threats, particularly those targeting consolidated digital infrastructure, is essential for a robust national cybersecurity strategy.

54. *See e.g.*, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 328–56 (Michael N. Schmitt ed., Cambridge Univ. Press 2017), https://doi.org/10.1017/9781316822524.020; U.N. Charter art. 2, ¶ 4, *https://www.un.org/en/about-us/un-charter/full-text* (last visited Dec. 3, 2024).

55. Cybersecurity Information Sharing Act of 2015, 6 U.S.C. §§ 1501–1510 (2015).

ICIT

CyberRisk
ALLIANCE

Task Force Members

Brett Freedman (CO-CHAIR)
Cory Simpson (CO-CHAIR)
Marene Allison
Edna Conway
Nick Anderson
Ankur Sheth