Testimony of Dr. David Bray, Chair of the Loomis Accelerator and Distinguished Fellow at the non-partisan Stimson Center before the House of Representatives, Judiciary Committee, Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet

Thursday, 18 September 2025

Chairman Issa, Ranking Member Johnson, and Members of the Subcommittee:

Thank you for the opportunity to testify today. I am Dr. David Bray, Chair of the Loomis Accelerator at the Stimson Center, Principal at LeadDoAdapt Ventures, Senior Advisor to the General Catalyst Institute, and a Fellow with the National Academy of Public Administration. I work on tech, data, and geopolitical issues to help:

- startups scale,
- communities adapt, and
- legacy organizations transform themselves amid rapid global changes.

My testimony focuses on advancing reliable, trustworthy AI consistent with the values of free societies and free markets from these perspectives.

I place my remarks in the context that the United States is experiencing multiple tech revolutions in addition to AI: advances in space tech, biotech, quantum tech, and the miniaturization of sensors and robots - all impacting U.S. companies, our workforce, and communities.

With respect to AI, I would like to mention three noteworthy advances to inform our discussion:

First, Active Inference AI models demonstrate faster learning and use less data and less energy. Such approaches can be bound by spatial or temporal limitations in ways that are human readable and interoperable across AI systems. Each of us as individuals could, in the future restrict, what AI systems do on our behalf.

Second, Open-Weight AI models with open-source code have shown we can transform currently complicated processes, such as a Veteran Affairs form, into a conversational interface, dramatically reducing time to complete and speeding access to care.

Third, Federated Learning allows AI systems to learn on datasets where they exist with proper consent, empowering both individuals and organizations to choose if their data sets and intellectual property are usable by AI - and negotiate a beneficial contractual relationship in return.

Given these advances, three guiding principles drive my recommendations to this subcommittee:

First principle: U.S. strategies for advancing AI should recognize interdependencies between AI and other tech advancements. This requires a light-touch policy framework. Recently, the National Academy of Public Administration has illuminated methods for sufficiently agile policy approaches to achieve measurable goals at the pace necessary given global changes.

Second principle: Different AI methods carry different risks and benefits. For example, AI approaches to computer vision and expert systems follow predictable outcomes, whereas generative AI produces less predictable results. As such, AI policies should reflect these differences in AI methods.

Third principle: There have been multiple waves of AI improvements over the years. We should expect continued advancements, which means U.S. policy approaches must adapt accordingly. For example, the Stimson Center's Loomis Council intentionally brings together industry leaders to adapt projects to new AI developments.

Even with different AI methods and the need for continuous adaptation, groups tied to specific domain applications of AI (for example: healthcare, transportation, finance) can promote data-level interoperability across AI systems, avoiding silos. When electronic health systems advanced in the 2000s, the U.S. encouraged the non-profit Health Level Seven to evolve an open standard framework for interoperable clinical data with privacy controls. We should do something similar now for health and AI. We each deserve a choice as to when an AI uses our data, and medical doctors should not be hindered by non-interoperable AI systems.

Given these principles, my recommendations are as follows:

First recommendation: Our policies should help advance freedom, human agency, and individual liberties. We face global competition from the Chinese Communist Party regarding AI's future, including their “AI+” initiative. U.S. AI strategy must simultaneously encourage the advancement of the entire U.S. AI industry - and encourage the industry to advance individual freedoms.

Second recommendation: Upgrading existing domain-specific laws is more pragmatic than attempting new, sweeping AI regulations. I recommend a domain-specific approach because the risks of different AI methods vary by application. Examples include updating the Privacy Act of 1974, revisiting HIPAA, and reviewing other existing laws where the speed, scale, and scope of AI methods impact different risk metrics. Congress’ recent efforts to update banking laws with respect to stablecoins is another example of updating existing statutes given new tech.

Third recommendation: Assess what actions, consistent with U.S. values of freedom, human agency, and individual liberties, may need light-touch policy to ensure AI efforts advance freedoms. We should build on Justice Brandeis's concept of the right to privacy, including individual choice about when personal data sets are (and are not) used by an AI. We should encourage industry to advance AI solutions that can operate on local devices that we could operate ourselves if we choose.

Any national AI strategy should ensure we don't stifle advancements toward reliable, trustworthy AI consistent with the values of both free societies and free markets.

Thank you, and I look forward to your questions.

Additional Materials Submitted as part of the Written Testimony

Topics:	Article:
On U.S. Export Controls tied to AI, and the Importance of "Red Teaming" the 2nd, 3rd Additional Consequences	01 - Hybrid AI and Human Red Teams_ Critical to Preventing Policies from Exploitation by Adversaries.pdf
On Companies Navigating the Complexities of Existing AI Rules, and Potential Solutions	02 - AI-Human Red Teaming article Dr David Bray
On Navigating AI's Impact on Education, Media, and Communities	03 - 7 leadership lessons for navigating the AI turbulence _ ZDNET
On Navigating AI's Impact on People, Companies, and the Workforce	04 - When deploying GenAI at scale, people must come first. Here's how _ ZDNET
On How Public and Private Boards Can Approach AI Governance	05 - Your board needs no-nonsense AI leadership - these experts explain why _ ZDNET
On How AI and Policies Can Help Advance Better Health and Healthcare Outcomes in the United States	06 - US-Healthcare-That-Works-Whitepaper
Lessons from Responding to 9/11 and the 2001 Anthrax Events, Why AI and Biology Require Us to Think Different	07 - Artificial Intelligence and Synthetic Biology Are Not Harbingers of Doom • Stimson Center
Commission on the Geopolitical Impacts of New Technologies and Data, including Trust in the Digital Economy	08 - GeoTech-Commission-Report-Full Commission on the Geopolitical Impacts of New Technologies and Data
Addendum - Two Examples of Positive Outcomes from AI Startups	09 - Addendum - Two Examples of Positive Outcomes from AI Startups
AI Services to Citizens in 2023 and Beyond - National Academy of Public Administration	10 - NAPA - AI Services to Citizens in 2023 and Beyond - National Academy of Public Administration
Public Sector Leadership, Helping Communities Adapt to a New Era - National Academy of Public Administration	11 - NAPA - Public Sector Leadership, Helping Communities Adapt to a New Era - National Academy of Public Administration

Topic: Technology Blog Brand: Techland Region: Americas
Tags: Artificial Intelligence, Rare Earth Elements, Red Teaming, Sanctions, Security, and Technology

Hybrid AI and Human Red Teams: Critical to Preventing Policies from Exploitation by Adversaries

February 28, 2025 | By: David Bray

SHARE:

Why such hybrid AI and human red teams are needed should now be clear.

The Red Cell series is published in collaboration with the Stimson Center. Drawing upon the legacy of the CIA's Red Cell—established following the September 11 attacks to avoid similar analytic failures in the future—the project works to challenge assumptions, misperceptions, and groupthink with a view to encouraging alternative approaches to

America's foreign and national security policy challenges. For more information about the Stimson Center's Red Cell Project, see here .

Red Cell

Despite the widespread belief among policymakers that geopolitical considerations alone are sufficient when developing technology policies and export controls, this view overlooks three crucial vulnerabilities that pose substantial risks to U.S. national security.

First, the accelerating pace of technological advancement has outpaced traditional geopolitical analysis frameworks. Just as the advent of steam engines created opportunities for new types of crime, like train robberies, today's technology policies, intended to protect U.S. technologies from exploitation, can be weaponized by adversaries—creating vulnerabilities more severe than the original threats they aimed to address.

Second, rigorous analysis of adversaries' capabilities in the formation of tech policies—a capability that was once a cornerstone of national security decisionmaking—has eroded. During the Cold War, the National Security Council (NSC) ultimately excelled at anticipating how adversaries might exploit U.S. tech policies, but recent decisions suggest this critical perspective is no longer a high priority—leaving the United States increasingly vulnerable to unintended consequences.

Third, modern AI systems offer an unprecedented opportunity to enhance analysis of adversaries' capabilities. These systems can rapidly generate multiple scenarios for how adversaries might weaponize proposed technology controls—similar to how financial institutions combine AI fraud detection systems with human analysis to identify and prevent complex financial crimes before they cause considerable damage. This suggests that policy formation should incorporate AI-enabled "red teaming" alongside human expertise to identify potential exploitation before policies are implemented. Traditionally, red teams in U.S. national security have provided alternative analysis and devil's advocacy by deliberately challenging consensus views and highlighting potential blind spots in intelligence assessments.

Why such hybrid AI and human red teams are needed should now be clear. Nations of concern have already found workarounds to well-intended and carefully constructed U.S. export controls or related technologies. Several prominent examples include:

1. **Iran's counter-exploitation of dual-use technology controls (2015-2020):** After U.S. export controls were imposed on dual-use technologies, Iran developed a sophisticated system of front companies and third-country intermediaries to circumvent these restrictions. Iran then used these same networks to help other nations facing similar restrictions, effectively creating a parallel market for controlled technologies. This network became so sophisticated that it began to undermine the effectiveness of U.S. export controls more broadly, as other nations learned to exploit the same pathways and mechanisms that Iran had developed.
2. **Russia's manipulation of International Traffic in Arms Regulations (ITAR) (2014-2018):** Following the implementation of U.S. ITAR restrictions on space technologies, Russia exploited these controls by positioning

itself as an alternative supplier of rocket engines to other nations. Russia specifically used the strict nature of U.S. ITAR controls to market its RD-180 rocket engines to European and Asian countries, arguing that Russia's technology had fewer restrictions and compliance burdens. This effectively reduced U.S. influence in the global space industry while increasing Russia's market share at that time.

3. **China's response to semiconductor controls (2022-2023):** After the United States imposed strict controls on advanced semiconductor exports, China responded by weaponizing its dominance in rare earth minerals, which are crucial for semiconductor manufacturing. China restricted exports of gallium and germanium, citing "national security" concerns. Beijing effectively turned the tables: it used the same regulatory framework the U.S. had established to protect U.S. technologies to create supply chain disruptions for Western manufacturers. This demonstrated how export controls can be mirrored and repurposed against their originators.

Strengthening export controls through AI-human red team analysis

New approaches are needed to complement the Committee on Foreign Investment in the United States' review process and other current criteria to determine how to best protect U.S. technologies, keep U.S. policy ahead of adversaries' rapidly evolving capabilities, and employ AI to strengthen the development of U.S. tech policies. A more effective approach to evaluating tech policies and possible export controls would involve hybrid "red teaming," a new policy using a combination of human and AI evaluations. Specifically, the new Trump administration could require that before any U.S. tech policy is issued, a combination of human and AI evaluation is performed to assess how state and nonstate adversaries could abuse any draft policy. Such an approach would:

- **Create a standing technology policy red team combining human expertise with AI capabilities.**
- **Restore adversarial analysis in NSC deliberations linked to considerations of how proposed export controls could be weaponized against U.S. interests.**
- **Mandate AI-enhanced red team analysis before implementing any new tech policy.**

In addition, the incorporation of AI-enhanced "red teaming" into U.S. technology policy formation would streamline the process. Instead of sequential reviews by different departments, AI-enhanced systems could help humans generate holistic analyses that consider multiple perspectives simultaneously. A hybrid human and AI team could simultaneously analyze multiple scenarios and provide comprehensive insights to all relevant stakeholders. The reduction in bureaucratic back-and-forth among agencies would be substantial.

For example: When evaluating export controls on quantum computing technologies, the AI system could simultaneously assess supply chain vulnerabilities, potential adversarial responses, and alternative sourcing options, providing a unified analysis that traditionally would require multiple rounds of interagency consultation. Human "red teamers" involved in the process could work to ensure that AI did not miss any new, important considerations given the amorphous nature of today's world.

In addition, a focused, hybrid human and AI team could continuously monitor global supply chain dynamics, identifying emerging vulnerabilities before they become critical issues. For example, if an adversary began establishing front companies to circumvent export controls, the AI system could help humans detect unusual patterns in corporate registrations, international transactions, and shipping routes that might escape human attention. This proactive identification of supply chain risks would allow policymakers to address vulnerabilities before they could be exploited, rather than reacting to problems after they occur.

Implementing This Approach

A standing technology policy red team combining human expertise with AI capabilities would modernize U.S. technology policy evaluation and help the United States avoid exploitation of its new technologies. This hybrid approach would pair AI's data processing and pattern recognition abilities with human strategic expertise to analyze potential policy impacts. For example, when evaluating semiconductor export controls, AI could rapidly assess global supply chains and simulate adversarial responses, while human experts could evaluate diplomatic implications. This integration with NSC deliberations would ensure comprehensive analysis of how proposed controls might be weaponized against U.S. interests.

The resulting mandatory AI-enhanced red team analysis would provide systematic protection against the potential unintended consequences of new technologies and export controls, including exploitation by adversaries. Before implementing controls on technologies like quantum computing, AI simulations could identify potential loopholes while human analysts assess real-world implications. This approach offers key benefits: better prediction of potential misuse of U.S. technologies, stronger protection of U.S. tech advantages, and more adaptive policymaking. The AI-human partnership would create a more sophisticated approach to technology policy development, ultimately strengthening U.S. national security while reducing the risk of policies backfiring.

The Trump administration has an opportunity to institutionalize this approach. By combining human expertise with AI-powered analysis, policymakers can identify potential vulnerabilities before policies are implemented rather than after they have been weaponized by adversaries. This approach would be particularly valuable for policies involving:

- **Export controls on advanced semiconductors:** The implementation of hybrid human and AI "red teaming" for semiconductor export controls would enable rapid assessment of global supply chains and potential circumvention tactics by adversaries. This was particularly evident in early December 2024, when China responded to U.S. semiconductor controls by weaponizing its dominance in rare earth minerals specifically restricting gallium and germanium exports. The combination of AI analysis and human expertise could have predicted and prepared countermeasures for such retaliatory actions, while also identifying alternative supply chain solutions before implementing the controls.
- **AI development and deployment restrictions:** A hybrid human and AI team could analyze multiple scenarios simultaneously to identify potential exploitation of AI development restrictions, while human experts evaluate the diplomatic and practical implications of these controls. The hybrid approach would help prevent repeat situations akin to when Iran used sophisticated networks of front companies to circumvent restrictions that happened when Tehran explored U.S. export controls on dual-use technologies in 2015-2020. This comprehensive analysis would enable policymakers to craft more robust AI deployment restrictions that anticipate and prevent exploitation methods before they emerge.

- **Data localization requirements:** A standing technology policy red team could continuously monitor and assess the effectiveness of data localization requirements across different jurisdictions and scenarios. The AI component could rapidly process global compliance patterns and identify potential vulnerabilities, while human analysts evaluate the geopolitical implications and practical feasibility of implementation. This approach would help prevent situations where adversaries could exploit gaps in data localization policies to gain unauthorized access to sensitive information.
- **Technology transfer limitations:** Drawing lessons from Russia's manipulation of ITAR regulations, hybrid human and AI "red teaming" could identify potential alternative markets and suppliers that might emerge in response to technology transfer limitations. The system could simultaneously analyze supply chain vulnerabilities, potential adversarial responses, and alternative sourcing options, providing a unified analysis that traditionally would require multiple rounds of interagency consultation. Human "red teamers" would ensure that emerging concerns and changing global dynamics are factored into the analysis, creating more effective and adaptable technology transfer policies.
- **Critical infrastructure protection measures:** A hybrid human and AI team could help identify interconnected vulnerabilities in critical infrastructure systems while simulating various attack scenarios in which adversaries could exploit these weaknesses. The hybrid human-AI team could continuously monitor global threats to critical infrastructure, detecting unusual patterns in corporate registrations, international transactions, and potential infiltration attempts that might escape human attention alone. As noted, this proactive identification of risks would allow policymakers to implement protective measures to U.S. technology policies before vulnerabilities can be exploited, rather than reacting to problems after they occur.

Cumulatively, implementing such solutions might be as straightforward as requiring every proposed U.S. technology policy to undergo a combined human-AI adversarial analysis focused on potential exploitation by state and nonstate actors. This would improve the need for "band-aid" solutions that could create more significant long-term vulnerabilities than the problems they attempt to solve.

In sum, the Trump administration has an opportunity to create more effective technology policies and export controls while streamlining their development through a combination of human and AI "red teaming." Given past misuses and abuses of well-intended U.S. export controls, the time is ripe for such improvements that will transform how the United States anticipates and responds to potential threats.

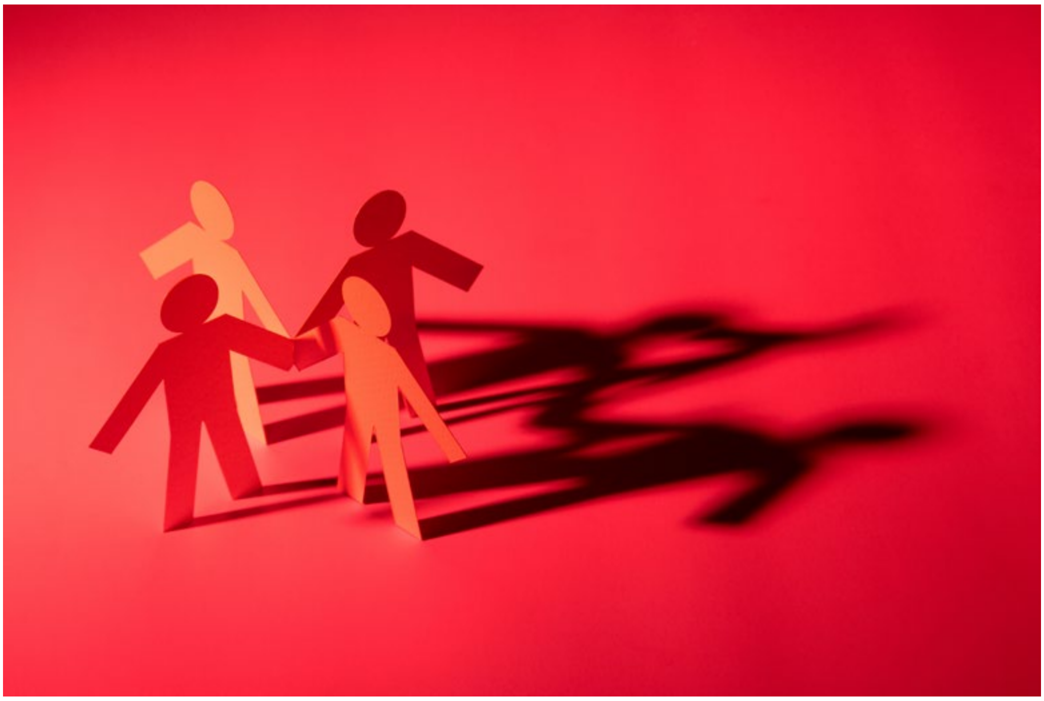
About the author: David Bray

David Bray is Chair of the Accelerator at the Alfred Lee Loomis Council and a Distinguished Fellow at the Stimson Center.

Image: humphery / Shutterstock.com

AI-human hybrid red teaming: A new paradigm for trade compliance and supply chain resilience

Against a backdrop of a rapidly shifting global trade environment, AI-human 'red teaming' – challenging compliance procedures and systems head-on – can be a valuable tool for kicking the proverbial tyres, not only for government but also potentially for industry, writes Dr David Bray.



In today's rapidly evolving global trade environment, compliance professionals face unprecedented challenges. The convergence of geopolitical tensions, technological disruption and regulatory proliferation has created a landscape where traditional compliance approaches increasingly fall short. Companies operating across borders must navigate a complex web of export controls, sanctions regimes, and supply chain vulnerabilities that can change with little warning. As regulatory frameworks become more sophisticated and enforcement more stringent, organisations need new methodologies to anticipate risks before they materialise. This article explores how AI-human hybrid red teaming offers a powerful new paradigm for proactive trade compliance and supply chain resilience.

The concept of red teaming – deliberately challenging assumptions and testing systems by adopting an adversarial mindset – has long been employed in military and cybersecurity contexts. Recent security research highlights that hybrid approaches combining human expertise with artificial intelligence capabilities represent the next frontier in anticipatory governance and risk mitigation. This methodology is now proving equally valuable in the trade compliance domain, where the stakes of failure include not only significant financial penalties but also reputational damage, supply chain disruptions, and potential national security implications.

The concept of 'red teaming' has long been employed in military and cybersecurity contexts. Recent security research highlights that hybrid approaches combining human expertise with artificial intelligence capabilities represent the next frontier in anticipatory governance and risk mitigation.

The evolving trade compliance landscape

The trade compliance landscape of 2025 bears little resemblance to that of even five years ago. Regulatory frameworks have grown increasingly complex, with jurisdiction overlaps creating compliance challenges that defy simple solutions. The United States, European Union, United Kingdom, and other major economies have expanded their export control regimes to encompass emerging technologies with dual-use applications, from advanced semiconductor manufacturing equipment to quantum computing components and synthetic biology tools. Meanwhile, sanctions programmes have become more targeted and sophisticated, focusing on specific sectors, technologies, and even individual supply chain nodes rather than broad country-wide restrictions.

This evolution reflects growing concerns about technology transfer, intellectual property protection, and national security in an era of strategic competition. Regulatory authorities have responded with more frequent updates to controlled items lists, enhanced enforcement mechanisms, and increased penalties for non-compliance. Regulatory authorities in the United States and other major economies are issuing updates and new rules with increasing frequency, often in response to rapid technological advancements and shifting geopolitical dynamics. This evolving landscape requires companies to remain vigilant and adaptable, as compliance programmes must now anticipate and respond to a near-constant stream of regulatory developments.

Why hybrid AI-human red teams are essential: learning from past failures

The necessity for hybrid AI and human red teams becomes evident when examining how nations of concern have historically circumvented carefully constructed export controls. Several prominent examples illustrate the sophisticated methods employed to undermine these regulatory frameworks:

Iran's counter-exploitation of dual-use technology controls (2015-2020): Following the imposition of US export controls on dual-use technologies, Iran developed an elaborate network of front companies and third-country intermediaries to bypass these restrictions. What made this particularly concerning was Iran's subsequent sharing of these evasion methodologies with other restricted nations, effectively creating an alternative market for controlled technologies. This network became so sophisticated that it began to undermine the broader effectiveness of US export controls, as multiple nations learned to exploit the same vulnerabilities and pathways.

Russia's manipulation of International Traffic in Arms Regulations (2014-2018): After the implementation of ITAR restrictions on space technologies, Russia strategically positioned itself as an alternative supplier of rocket engines. Russian authorities specifically leveraged the strict nature of US ITAR controls as a marketing advantage for their RD-180 rocket engines, emphasising to European and Asian countries that Russian technology carried fewer restrictions and compliance burdens. This approach effectively diminished US influence in the global space industry while expanding Russia's market share during this period.

China's response to semiconductor controls (2022-2023): When the United States imposed stringent controls on advanced semiconductor exports, China responded by weaponising its dominance in rare earth minerals critical for semiconductor manufacturing. Beijing restricted exports of gallium and germanium, citing 'national security' concerns - effectively mirroring the same justification used by the United States. This demonstrated how export controls can be repurposed against their originators, creating supply chain disruptions for Western manufacturers and highlighting the vulnerability of even well-designed regulatory frameworks.

> **This hybrid approach addresses a fundamental limitation of purely AI-driven compliance tools: their inability to fully understand the nuanced geopolitical, commercial, and operational contexts in which trade compliance decisions are made.**

These examples underscore why traditional approaches to export control compliance are insufficient. Adversaries continuously evolve their evasion tactics, exploiting regulatory blind spots and leveraging global supply chain complexities. AI-human hybrid red teams can simulate these adaptive adversarial behaviours, identifying potential vulnerabilities before they can be exploited in the real world.

Understanding AI-human hybrid red teaming

At its core, AI-human hybrid red teaming combines the creative problem-solving and contextual understanding of human experts with the pattern recognition, data processing, and scenario modelling capabilities of artificial intelligence systems. Unlike traditional compliance audits that focus on historical performance against established requirements, red teaming adopts an adversarial mindset to identify potential vulnerabilities and exploitation pathways.

Security experts note that the most effective red teams leverage both human creativity and AI's analytical power, creating a synergy that exceeds what either could accomplish independently. In the trade compliance context, this means bringing together compliance professionals, legal experts, and supply chain specialists with advanced AI systems trained on global regulatory frameworks, trade data, and risk patterns.

The AI component can rapidly process vast amounts of regulatory information, transaction data, and supply chain intelligence to identify patterns and anomalies that might escape human attention. For example, an AI system might detect unusual shipping patterns that suggest potential transshipment to evade sanctions, or identify correlations between seemingly unrelated regulatory changes that could impact a company's operations. The human component provides critical judgment, contextual understanding and creative thinking to interpret these findings, develop realistic scenarios, and design effective mitigation strategies.

This hybrid approach addresses a fundamental limitation of purely AI-driven compliance tools: their inability to fully understand the nuanced geopolitical, commercial, and operational contexts in which trade compliance decisions are made. Industry experts note that manual AI red teaming offers the benefit of human creativity, while automated tools make it possible to red team at scale. The most effective approach combines both elements, leveraging technology to enhance rather than replace human expertise.

Implementing AI-human hybrid red teams for trade compliance

Implementing an effective AI-human hybrid red team for trade compliance requires careful consideration of team composition, methodological approach, and technological infrastructure. The most successful implementations typically include the following elements:

1. **Multi-disciplinary expertise**: Effective red teams bring together professionals with multi-disciplinary backgrounds and perspectives. This might include trade compliance specialists, legal experts, supply chain managers, data scientists and geopolitical analysts. This diversity enables the team to consider multiple dimensions of risk and develop more comprehensive testing scenarios.
2. **Advanced AI capabilities**: The AI component should include capabilities for natural language processing (to analyse regulatory texts and identify implications), anomaly detection (to identify unusual patterns in trade data), predictive analytics (to anticipate regulatory trends), and scenario modelling (to test the impact of potential changes). These capabilities can be developed in-house or accessed through specialised platforms available in the market.
3. **Structured methodology**: Red teaming exercises should follow a structured methodology that includes scenario development, vulnerability identification, exploitation testing, and mitigation planning. This ensures that exercises are comprehensive, reproducible, and yield actionable insights.
4. **Executive support**: Successful red teaming requires strong executive support and a culture that values constructive challenges. Leadership must understand that the purpose is not to assign blame for vulnerabilities but to identify and address them before they can be exploited.

5. Continuous learning: Both the human and AI components of the red team should engage in continuous learning, with findings from each exercise informing future scenarios and testing approaches. This creates a virtuous cycle of improvement that enhances the organisation's overall compliance posture.

Industry applications of AI-human hybrid red teaming

While AI-human hybrid red teaming for trade compliance is still an emerging practice, several industries could implement this approach to address their specific compliance challenges:

1. High-tech manufacturing industry applications

A semiconductor manufacturer with global operations could implement an AI-human hybrid red team to strengthen its export control compliance programme. The AI system would continuously analyse global semiconductor trade data, regulatory changes affecting controlled technologies, and emerging geopolitical tensions that might signal new restrictions. Human experts would then develop scenarios testing the company's classification processes, deemed export controls, and supply chain security.

For example, the team might simulate a scenario where a foreign entity attempts to acquire controlled semiconductor manufacturing equipment through a series of seemingly unrelated transactions across multiple jurisdictions. The AI component would flag unusual patterns in customer inquiries and order placements, while human experts would develop plausible exploitation pathways based on their understanding of industry practices and regulatory blind spots. This approach would enable the company to identify and address vulnerabilities in its transaction screening processes before actual adversaries could exploit them.

2. Financial services industry applications

A global financial institution could deploy an AI-human hybrid red team to test its sanctions compliance programme. The AI component would analyse global payment patterns, beneficial ownership data and regulatory enforcement trends to identify potential vulnerability patterns. Human experts would then develop scenarios simulating sophisticated sanctions evasion attempts that exploit these vulnerabilities.

The team might create a scenario where sanctioned entities attempt to access the global financial system through a complex network of shell companies, intermediaries and cryptocurrency transactions. The AI system would identify subtle connections between seemingly unrelated entities and transactions, while human experts would develop realistic evasion strategies based on their understanding of financial regulations and criminal methodologies. This approach would enable the institution to strengthen its customer due diligence processes, transaction monitoring systems, and beneficial ownership verification procedures.

The AI system would analyse the company's global supply chain data, research collaborations, and regulatory developments affecting pharmaceutical ingredients and technologies. Human experts would then develop scenarios testing the company's compliance controls against sophisticated exploitation attempts.

3. Pharmaceutical industry applications

A pharmaceutical company with global research and manufacturing operations could implement an AI-human hybrid red team to assess its vulnerability to emerging export control and sanctions risks. The AI system would analyse the company's global supply chain data and research collaborations, as well as regulatory developments affecting pharmaceutical ingredients and technologies. Human experts would then develop scenarios testing the company's compliance controls against sophisticated exploitation attempts.

For instance, the team might simulate a scenario where a restricted entity attempts to acquire controlled pharmaceutical manufacturing technology through a series of research collaborations and licensing agreements. The AI component would identify unusual patterns in research inquiries and technology transfer requests, while human experts would develop plausible exploitation strategies based on their understanding of industry practices and regulatory frameworks. This approach would enable the company to strengthen its technology transfer controls, research collaboration screening processes, and supply chain security measures.

Key applications in trade compliance and supply chain resilience

AI-human hybrid red teaming offers value in several critical areas of trade compliance and supply chain management:

Export control classification: Determining whether items are subject to export controls and identifying the applicable classification can be challenging, particularly for emerging technologies and items with multiple potential applications. Red teams can develop scenarios testing classification methodologies against novel products or unusual use cases, identifying potential gaps in current approaches. Should an adversary begin establishing front companies to circumvent export controls, the AI system could help humans detect unusual patterns in corporate registrations, international transactions, and shipping routes that might escape human attention. This same approach can be applied to testing internal classification processes, with the AI component identifying potential misclassification patterns and human experts developing scenarios to test classification decision-making.

Sanctions compliance: Sanctions programmes are increasingly complex, with targeted restrictions that can change rapidly in response to geopolitical developments. Red teams can simulate potential sanctions scenarios, testing screening processes, beneficial ownership identification procedures and transaction monitoring systems against sophisticated evasion attempts. The hybrid approach is particularly valuable here, as AI systems can process vast amounts of relationship data to identify potential sanctions exposure, while human experts can develop realistic scenarios based on their understanding of geopolitical trends and regulatory priorities.

Supply chain resilience: Beyond compliance considerations, AI-human hybrid red teaming can help organisations assess the overall resilience of their supply chains to regulatory disruptions. By simulating potential export control changes, sanctions designations or forced divestment requirements, red teams can identify critical vulnerabilities and develop contingency plans. Recent research highlights that this approach enables proactive identification of supply chain risks before they materialise into actual disruptions. The AI component can model complex supply chain interdependencies and simulate cascade effects from regulatory changes, while human experts can develop realistic scenarios based on geopolitical understanding and industry knowledge.

Deemed export compliance: Controls on technology transfers to foreign nationals (deemed exports) present compliance challenges in multinational organisations. Red teams can develop scenarios testing access controls, training effectiveness, and monitoring systems against sophisticated exploitation attempts. The hybrid approach enables more comprehensive testing, with AI systems analysing access patterns and communication data while human experts develop realistic scenarios based on their understanding of technology transfer mechanisms and regulatory priorities.

Advanced persistent threat detection: In an era of increased 'grey zone conflict', organisations face sophisticated nation-state advanced persistent threats ('APTs') targeting their digital supply chains. AI-human hybrid red teams can simulate these threats by developing scenarios that test an organisation's ability to detect and respond to software compromises, hardware tampering, and data exfiltration attempts. In such a hybrid arrangement, the AI component can analyse software code, firmware and network traffic for anomalies that might indicate compromise, while human experts develop realistic attack scenarios based on known APT tactics. This approach is particularly valuable for organisations with complex digital supply chains involving multiple vendors, open-source components and international development teams, enabling them to identify and address vulnerabilities before sophisticated state-sponsored actors can exploit them.

Challenges and limitations

While AI-human hybrid red teaming offers significant advantages, implementing this approach effectively requires addressing several challenges:

1. **Data quality and availability**: Effective AI analysis depends on access to high-quality, comprehensive data on regulations, transactions and supply chain relationships. Organisations may need to invest in data integration and quality improvement initiatives to support red teaming activities.
2. **AI limitations**: Current AI systems have limitations in understanding context, making ethical judgments, and anticipating novel scenarios without a historical precedent. Human oversight and guidance remain essential to ensure that red teaming exercises produce meaningful, actionable insights.
3. **Organisational resistance**: Red teaming inherently involves challenging established practices and identifying potential weaknesses, which may encounter resistance in organisations with strong compliance cultures. Effective implementation requires careful change management and clear communication about the purpose and value of the approach.
4. **Resource requirements**: Implementing AI-human hybrid red teaming requires investment in technology, expertise, and ongoing programme management. Organisations must balance these costs against the potential benefits of enhanced compliance effectiveness and risk mitigation.
5. **Regulatory uncertainty**: The evolving nature of export controls creates challenges for red teaming exercises. Teams must develop scenarios that accommodate regulatory uncertainty, particularly for emerging technologies where frameworks remain in flux. Organisations need approaches that provide actionable insights despite this uncertainty.

Despite these challenges, the potential benefits of AI-human hybrid red teaming for trade compliance and supply chain resilience make it a worthwhile investment for organisations operating in complex global environments.

The future of AI-human hybrid red teaming

Several trends are likely to shape the evolution of AI-human hybrid red teaming for trade compliance:

- **Increased automation**: As AI capabilities advance, more aspects of the red teaming process will be automated, enabling more frequent and comprehensive testing with less manual effort. However, human oversight and creativity will remain essential for developing realistic scenarios and interpreting results.
- **Regulatory recognition**: Regulatory authorities may increasingly recognise proactive red teaming as evidence of compliance programme effectiveness, potentially offering incentives or penalty mitigation for organisations that implement robust testing programmes.
- **Collaborative approaches**: Industry consortia and public-private partnerships may emerge to share red teaming methodologies, findings and best practices, enhancing overall compliance effectiveness across sectors.
- **Integration with risk management**: AI-human hybrid red teaming will increasingly be integrated with broader enterprise risk management frameworks, enabling more comprehensive assessment and mitigation of interconnected risks.
- **Grey-zone conflict adaptation**: As geopolitical competition intensifies in the 'grey zone' between peace and conventional warfare, AI-human hybrid red teams will evolve to address increasingly sophisticated supply chain attacks targeting software, hardware, and data. Teams will develop capabilities to simulate nation-state-level threats that blend legitimate commercial activities with malicious intent.

Success in the future across these five trends will require enhanced collaboration amongst trade compliance, cybersecurity and counter-intelligence specialists, as well as AI systems capable of detecting subtle patterns across digital and physical supply chains. Organisations that develop these advanced red-teaming capabilities will gain significant advantages in protecting their operations against sophisticated adversaries operating below the threshold of traditional conflict.

Conclusion

In an era of increasing regulatory complexity and supply chain vulnerability, AI-human hybrid red teaming offers a powerful novel approach to trade compliance and risk management. By combining the analytical power of artificial intelligence with the contextual understanding and creativity of human experts, organisations can remedy regulatory issues, seize opportunities before competitors do, or shore up defences before adversaries exploit vulnerabilities.

As regulatory frameworks continue to evolve and enforcement intensifies, proactive approaches to compliance will become increasingly essential. Organisations that implement effective AI-human hybrid red teaming programmes will be better positioned to navigate this complex landscape, maintaining compliance while preserving operational flexibility and supply chain resilience.

The future of trade compliance lies not in reactive documentation and procedural adherence, but in proactive identification and mitigation of emerging risks. AI-human hybrid red teaming provides a methodology to achieve this future state, enabling organisations to stay ahead of regulatory developments and maintain a competitive advantage in an increasingly complex global environment.

Dr. David Bray is a Distinguished Fellow with the Stimson Center, Chair of the Accelerator at the Loomis Council, and previously Executive Director for two different bipartisan Commissions on tech, data and geopolitics.

WWW.STIMSON.ORG

7 leadership lessons for navigating the AI turbulence

Vala Afshar

zf L/Getty Images

In a recent episode of our weekly podcast DisrupTV, Constellation Research CEO Ray Wang and I assembled an extraordinary panel of leaders to discuss effective leadership in today's rapidly changing world. The conversation featured Ellen McCarthy, founder and CEO of the Trust in Media Cooperative; Lev Gonick, award-winning CIO of Arizona State University (ASU); and Dr. David Bray, Chair of the Accelerator and Distinguished Fellow at the Stimson Center.

The discussion revealed critical insights for CEOs, boards, and C-suite executives navigating today's complex leadership landscape. Here are the key takeaways from these seasoned leaders.

1. Embrace disruption as opportunity

ASU's Lev Gonick shared how the school has consistently turned moments of disruption into strategic advantages. During the 2008 economic crisis, rather than merely trying to survive, ASU positioned itself with what Gonick calls an "anti-fragile approach."

Also: 5 ways to escape middle management and fast-track your journey to the top

"We didn't just figure out how to survive the downturn but positioned ourselves to be better at the other end of it," Gonick explained. This strategy led to the creation of ASU Online, which started with just 400 students and now serves more than 104,000 students in nearly 400 programs.

For CEOs and boards facing disruptive forces, Gonick's experience at ASU offers a masterclass in strategic resilience. His approach demonstrates that organizational crises present rare opportunities to fundamentally reimagine business models rather than merely weathering the storm.

Executive leaders should note how ASU transformed the 2008 financial crisis into a catalyst for digital transformation, launching what would become a thriving online education platform. Similarly, when many organizations focused solely on survival during the pandemic, ASU partnered with entertainment industry leaders to create immersive learning experiences that improved student outcomes.

This anti-fragile mindset -- deliberately using disruption to become stronger -- represents a powerful strategic framework for C-suites and boards. Rather than treating disruptions as temporary challenges to overcome, forward-thinking executives should view them as inflection points to accelerate innovation and create sustainable competitive advantages that wouldn't be possible during periods of stability.

Leadership lesson 1: True leaders view disruption not as a threat but as a catalyst for transformation. The most successful organizations use periods of uncertainty to make bold, forward-thinking moves rather than retreating to defensive positions.

2. Information management in an era of overload

Trust in Media's Ellen McCarthy, drawing on her extensive intelligence community background, offered a six-point framework for leaders dealing with today's information ecosystem:

1. **Question everything without becoming cynical:** Not all sources are created equal. Just because something is trending doesn't mean it's true.
2. **Diversify information inputs:** Mix your data input like a good cocktail. In intelligence, whether for national security or business, it gets better when you blend sources.
3. **Use AI appropriately:** AI is like a smart intern -- helpful but not always right. It's a tool, and at the end of the day, it's about applying human judgment.
4. **Embrace diverse perspectives:** Surround yourself with people who have different perspectives. It's always easier to manage people who think alike, but what comes out of managing diverse backgrounds and thoughts is a thing of beauty.
5. **Prioritize simplicity:** If you can't explain what you're doing in one sentence or a single PowerPoint slide, you're done.
6. **Remember the human factor:** Data is incredibly powerful, but intelligence is only as good as your understanding of people -- their motives, fears, and desires.

McCarthy's framework offers a practical roadmap for CEOs and boards navigating today's complex information landscape. Executive leaders must cultivate a culture of healthy skepticism without falling into cynicism, ensuring their organizations can distinguish signal from noise.

Also: Business leaders are embracing AI, but their employees are not so sure

They should institutionalize processes that triangulate information from diverse sources, much like intelligence agencies do, while implementing AI tools as supplements to -- not replacements for -- human judgment. Similarly, corporate boards should seek cognitive diversity in their composition and executive teams, valuing the friction that comes from different perspectives. C-suite communications should prioritize clarity and simplicity, particularly when conveying complex strategies.

Finally, executives must remember that behind every data point and market trend are human motivations and behaviors -- understanding these remains the ultimate competitive advantage in an increasingly automated world.

Leadership lesson 2: In an age of information overload, leaders must develop robust frameworks for evaluating information quality while maintaining human judgment at the center of decision-making.

3. Lead through multiple simultaneous revolutions

The Stimson Center's David Bray highlighted that we're not just experiencing an AI revolution but multiple simultaneous revolutions -- in quantum computing, commercial space, synthetic biology, and personalized medicine.

"Usually, when just one revolution happens, there's tremendous social and business upheaval, but we're doing five or six in parallel," Bray noted. This creates unprecedented challenges for leaders. Bray emphasized that traditional leadership approaches won't work in this environment: "You can't reach for those old levers that you used to -- they won't work. You've got to have new levers and new strategies that involve communities from the bottom up, involve decentralized approaches, and at the same time work to pull people together."

Also: How to use ChatGPT: A beginner's guide to the most popular AI chatbot

Bray's analysis presents both a warning and an opportunity for CEOs and boards. The convergence of AI, quantum computing, commercial space, synthetic biology, and personalized medicine creates a business environment without historical precedent. Executive leaders must recognize that these technologies aren't merely tools to optimize existing business models but catalysts for entirely new paradigms.

In addition, corporate boards should evaluate their organizations' readiness not just for one technological shift but for cascading and compounding disruptions across multiple domains. This requires fundamentally rethinking strategic planning horizons, talent development, and organizational structures. The most forward-thinking executives are already moving beyond traditional top-down leadership models toward more adaptive, networked approaches that can harness collective intelligence while maintaining strategic coherence. As Dr. Bray emphasizes, the old playbooks for managing change simply won't suffice in this new era of simultaneous revolutions.

Leadership lesson 3: Today's leaders must recognize that we're in a period of multiple overlapping revolutions, requiring entirely new approaches to leadership that embrace decentralization while fostering unity.

4. Build trust in a fractured information landscape

McCarthy explained how the broken information ecosystem presents both challenges and opportunities for leaders. "Our information ecosystem is broken. On one hand, it's amazing because pretty much everything you could ever need is there, but it's very hard to get to it." McCarthy said. "The volume of information is just so overwhelming."

Also: 3 ways AI can unlock new (and better) changes for your business

Rather than telling people what to believe, McCarthy advocates for providing frameworks that help people assess information quality themselves. "I'm not going to tell you whether to trust something, but I believe, like in making food choices, I know when to eat a Big Mac when I'm on the road, and I know when to eat organic chicken when I'm trying to lose weight. Give people the same agency to make those decisions for themselves."

Leadership lesson 4: Effective leaders don't dictate truth but build systems that empower people to make informed judgments, fostering both trust and agency.

5. Education and leadership in the AI era

Gonick shared ASU's approach to AI, emphasizing that educational institutions must lead in preparing students for an AI-first world. "If our job in the overall pipeline of human capital development is to prepare folks for the next parts of their lives, it's incumbent on us to prepare students in an intentional way," Gonick explained. This means developing new degrees, integrating AI tools across all subjects, and forming partnerships to prepare public agencies to be "AI-first agencies."

Leadership lesson 5: Forward-thinking leaders must adapt their organizations to emerging technologies and actively prepare their teams and stakeholders for a fundamentally different future.

6. Bottom-up leadership for complex challenges

All three panelists emphasized the importance of bottom-up, community-driven approaches to leadership. McCarthy articulated this philosophy succinctly: "A leader's job is to set a vision, make sure everybody's on board with it, and then equip everyone to be able to do it. It's not about doing it yourself."

Also: 3 ways AI can unlock new (and better) changes for your business

She outlined three key leadership actions: "Educate, equip, and empower. Make sure they understand where you're going. Make sure they're on board with it. Listen to them. Make sure they have everything they need -- the tools, the framework, whatever it is -- and then let them go."

Leadership lesson 6: In complex environments, effective leadership means creating the conditions for distributed problem-solving rather than centralized control.

7. Create narratives that unite

Bray highlighted perhaps the most critical leadership challenge today: "We are lacking a large enough narrative or big enough tent that people can see themselves in. There's a very real risk that with all these technologies, we just become more isolated, we become more lonely." He noted that many people are experiencing anxiety because traditional social contracts have broken down: They thought the deal was, I go to school once, and I have a job that's the same job for the next 40 years. That's no longer the case.
Leadership lesson 7: Today's most effective leaders create inclusive narratives that help people make sense of rapid change and see themselves as part of a positive future.

The path forward

The conversation that these three luminary leaders had revealed that leadership in turbulent times requires a delicate balance: Embrace disruption while providing stability, leverage technology while preserving human judgment, and distribute authority while maintaining cohesion. As organizations navigate multiple simultaneous revolutions, leaders who can create inclusive narratives, build trust through transparency, and empower bottom-up problem-solving will be best positioned to thrive.

Also: AI won't take your job, but this definitely will

These insights suggest that the most successful leaders will be those who can help their organizations not just survive disruption but use it as a catalyst for transformation -- turning periods of uncertainty into opportunities for reinvention and growth.

This article was co-authored by Dr. David Bray, principal and CEO at LeadDoAdapt (LDA) Ventures, chair of the Accelerator, and distinguished fellow at the Stimson Center.

*Want more stories about AI? **Sign up for Innovation**, our weekly newsletter.*

ZDNET

Why you can trust ZDNET: **Our process**

Home / Business

When deploying GenAI at scale, people must come first. Here's how

'Deployment empathy' means managing change thoughtfully, creating psychological safety, reassuring anxious workers, and collaborating to co-create solutions tailored for shared benefit. Three business leaders break it down.

Written by **Vala Afshar,** Contributing Writer

March 22, 2024 at 12:50 p.m. PT

FG Trade/Getty Images

A recent Salesforce survey of 600 IT leaders reveals a new mandate from their bosses: Incorporate generative artificial intelligence (GenAI) into the technology stack -- and fast. But the response from IT professionals is "not so fast" -- highlighting concerns about resources, data security, and data quality.

Also: Even more businesses will use AI and data to boost sales and services this year

Nearly three in five IT professionals say business stakeholders hold unreasonable expectations regarding the speed and agility of new technology implementations. In fact, the IT leadership survey reveals almost nine in 10 IT professionals can't support the deluge of AI-related requests they receive at their organization.

A 2024 study found that 90% of IT leaders say it's tough to integrate AI with other systems. AI adoption has exploded and amplified the need for a coherent IT strategy, but achieving that balance is easier said than done. MuleSoft's ninth annual Connectivity Benchmark Report was produced from interviews with 1,050 IT annual Connectivity Benchmark Report was produced from interviews with 1,050 IT leaders (management positions or above) across the globe (public and private sector with at least 1,000 employees). The report's executive summary suggests:

- **The new normal: AI inflection point amplifies the need for a coherent IT strategy**. Eighty-seven percent of IT leaders report that the nature of digital transformation is changing. AI further complexifies the tech landscape, with 991 apps in the average enterprise. IT budgets increase to meet the surging demand.
- **AI adoption explodes, integration and security concerns are the biggest barriers.** The AI genie is out of the bottle, with over three-quarters of organizations reporting they use multiple AI models. As many as 90% say difficulty integrating AI with other systems is a barrier, followed by 79% reporting security concerns.
- **IT leaders acknowledge that data silos and systems fragility are holding their companies back.** Almost universal, 98% of IT leaders report facing challenges regarding digital transformation. Key drivers are the persistence of data silos at 81% and the fragility of tightly coupled and highly dependent systems at 72%.

Business success and growth is dependent upon trust, data, AI and automation. Businesses today are competing in an experience-led economy that is based on trust, personalization, speed, and intelligence. Most people are concerned about the implications of GenAI on data security, ethics, and bias. In fact, 81% of customers want a human to be in the loop, reviewing and validating generative AI outputs. The road to implementation and adoption of AI in a secure, trustworthy, scalable and stakeholder value-driven model will require a lot more than just solid technology and processes. What's needed most is "deployment empathy."

Also: Will AI hurt or help workers? It's complicated

To better understand how large, complex organizations successfully deploy and adopt new technologies in order to turbo charge their value creation capabilities, Constellation Research CEO Ray Wang and I invited three business technology leaders to our weekly podcast DisrupTV. We discussed GenAI -- and the need for organizations to adopt and practice deployment empathy when launching new AI efforts -- with Teresa Carlson, Rhonda Vetere, and Dr. David Bray.

Deployment empathy embodies putting people first, managing change thoughtfully, creating psychological safety, reassuring anxious workers, and collaborating across sectors to co-create solutions tailored for shared benefit. The practice of deployment empathy centers around the principle that empathetic leadership will enable a smooth, productive transition amid the disruption created by GenAI's impacts on companies, customers, employees, citizens, communities, and societies.

Teresa Carlson is a technology executive and leader with more than 20 years of experience helping governments and enterprises adopt new technologies like cloud computing and AI. Teresa started and led Amazon Web Services' worldwide public sector business, helping more than 5,000 government agencies and 10,000 education institutions adopt cloud technologies. She also served as president and chief commercial officer at Flexport, a supply chain/logistics company; corporate vice president of Microsoft, as well president and chief growth officer at Splunk.

Currently, Teresa is a strategic advisor to technology companies and government organizations. She serves on the boards of Finch AI, Cura, and others. Teresa is also vice chair of the White House Historical Association and an Atlantic Council board member.

We cannot overemphasize the critical importance of radical collaboration between public and private sector entities when working to adopt emerging technologies like AI in government settings.

This entails deeply listening to agencies' specific needs, co-designing responsible solutions tailored for them, and ensuring full interoperability with legacy systems.

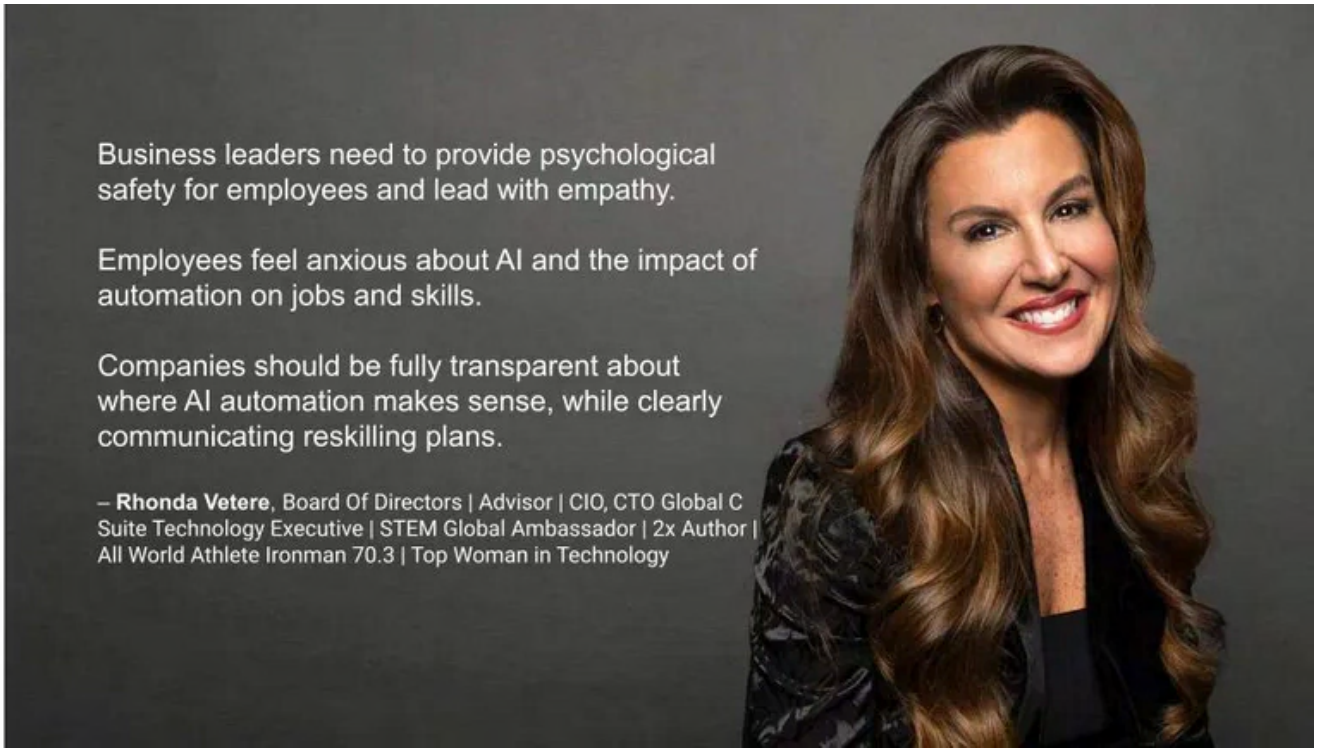
– **Teresa Carlson**, General Catalyst Advisor, Board Member, Investor and Vice-Chair White House Historical Association

Vala Afshar

During the lively group discussion, Teresa emphasized the critical importance of radical collaboration between public and private sector entities when working to adopt emerging technologies like AI in government settings. This entails deeply listening to agencies' specific needs, co-designing responsible solutions tailored for them, and ensuring full interoperability with legacy systems.

Also: Want to work in AI? How to pivot your career in 5 steps

Why is deployment empathy so essential? Government and enterprise environments do not reward risk-taking and innovation. Championing deployment empathy requires recognizing the current risk-reward environment. Leaders in these risk-averse cultures must create incentives and psychological safety for teams to feel comfortable trying new things like AI. This involves transparency, setting clear guidelines, and managing change thoughtfully.



Business leaders need to provide psychological safety for employees and lead with empathy.

Employees feel anxious about AI and the impact of automation on jobs and skills.

Companies should be fully transparent about where AI automation makes sense, while clearly communicating reskilling plans.

– **Rhonda Vetere**, Board Of Directors | Advisor | CIO, CTO Global C Suite Technology Executive | STEM Global Ambassador | 2x Author | All World Athlete Ironman 70.3 | Top Woman in Technology

Vala Afshar

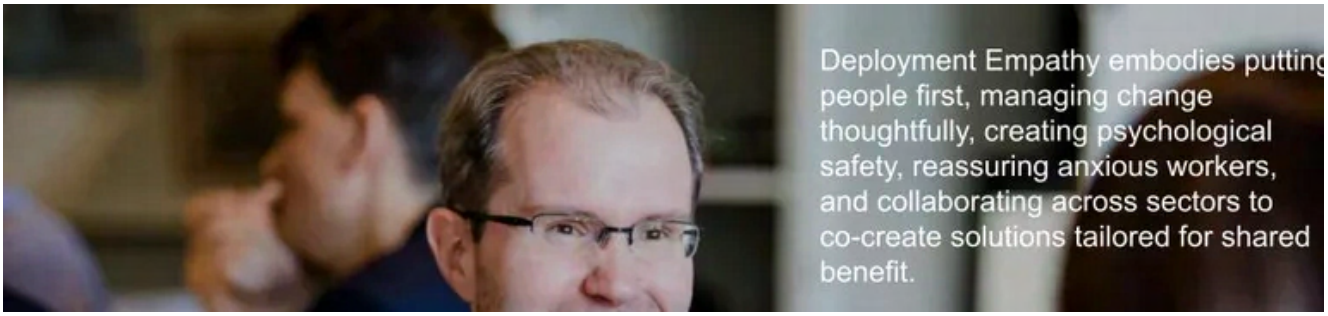
Also bringing deep technology and leadership expertise, Rhonda Vetere is a global executive who has led major digital transformation initiatives across industries. She is also an accomplished triathlete and author who applies athletic approaches to business leadership and strategic advisory roles. She has worked as a CIO, CTO, and digital transformation leader at large companies like HP Enterprise, Barclays, and JPMorgan.

She is the author of the book "Grit and Grind: 10 Principles for Living an Extraordinary Life," which focuses on achieving one's full potential. Rhonda serves on boards and is a strategic advisor to companies globally on digital transformation and emerging technologies like AI.

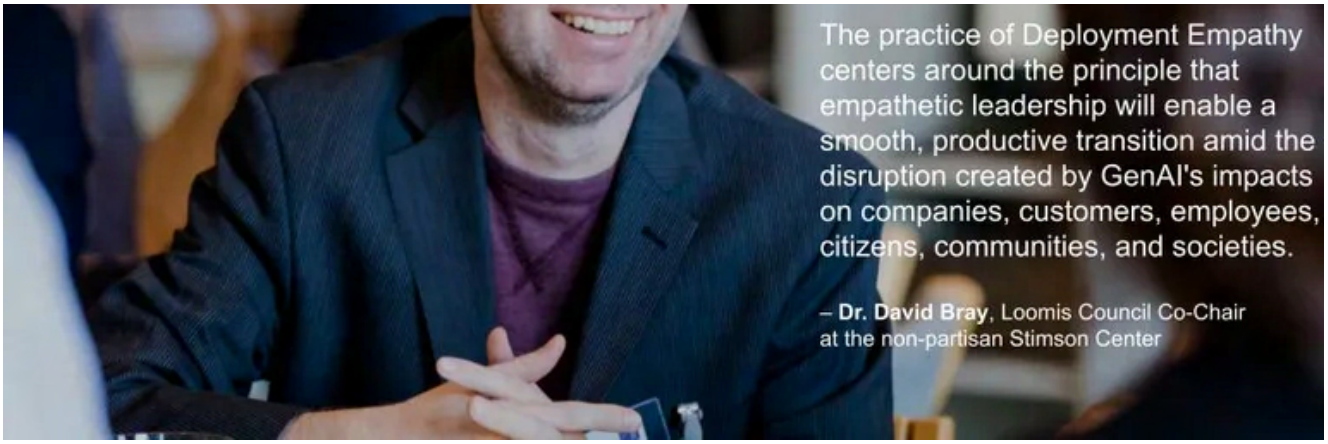
> Trust in AI technology and the companies that develop it is dropping. Globally, trust in AI companies has dropped to 53%, down from 61% five years ago. In the U.S., trust has dropped 15 percentage points (50% to 35%) over the same period.https://t.co/qsqkZxzQcg
>
> — Vala Afshar (@ValaAfshar) March 8, 2024

As part of the discussion, Rhonda noted that many employees feel anxious about AI automation's potential impact on jobs and skills. Business leaders should be fully transparent about where AI automation makes sense while clearly communicating reskilling plans.

Why is deployment empathy needed now? When deploying AI, leaders should start conversations by discussing where humans fit into the process rather than leading with the technology. Championing AI adoption requires a human-centric mindset focused on impact to people and jobs - deployment empathy.



Deployment Empathy embodies putting people first, managing change thoughtfully, creating psychological safety, reassuring anxious workers, and collaborating across sectors to co-create solutions tailored for shared benefit.


The practice of Deployment Empathy centers around the principle that empathetic leadership will enable a smooth, productive transition amid the disruption created by GenAI's impacts on companies, customers, employees, citizens, communities, and societies.

– **Dr. David Bray**, Loomis Council Co-Chair at the non-partisan Stimson Center

Dr. David Bray, Loomis Council Co-Chair at the non-partisan Stimson Center

Vala Afshar

As part of the discussion trio, Dr. David Bray is an acclaimed technology leader with extensive experience guiding organizations through complex, high-risk situations. He is an award-winning, recognized expert on issues such as leadership during turbulent times, digital transformation, resilience, countering disinformation, and responsible adoption of emerging technologies like AI.

He has served in multiple leadership roles dealing with crisis situations and challenges, including bioterrorism preparedness and response, leading two bipartisan National Commissions on R&D, as well as work with the US intelligence cmmunity, the FCC, and the Department of Defense. David is co-chair for the Loomis Council and distinguished fellow at the Stimson Center.

Also: Workers with AI skills can expect higher salaries - depending on their role

David observed that AI and related technologies are catalyzing seismic societal changes in how we work and live, at a pace exceeding our ability to adapt policies, social contracts, and organizational change management practices. He noted that this calls into question existing social contracts around displaced workers and economic opportunity, which is why leadership paired with deployment empathy in our GenAI era is important now more than ever.

How to embody deployment empathy authentically? David noted that leaders must provide a steady "non-anxious presence" amidst uncertainty to reassure people worried about job loss. This empathetic leadership is crucial. He also noted AI worried about job loss. This empathetic leadership is crucial. He also noted AI journeys for companies, governments, and society will involve both short-term sprints and longer-term marathons. While moving fast, leaders cannot forgo security, customer value, and business continuity. We must balance thoughtfulness, empathy, and care for people with the urgency to innovate for shared prosperity.

During the discussion, Teresa highlighted the need for clear governance frameworks and guidelines around ethical, fair, transparent, and legally compliant AI deployment in the public sector. This responsible AI approach builds trust and mitigates risks as government agencies adopt AI.

Rhonda also suggested creating formal programs to identify roles needing upskilling, "ringfencing" those employees, providing educational resources, and guaranteeing jobs after reskilling is complete. This thoughtful change management reduces anxiety and distrust, while promoting psychological safety.

Also: Beyond programming: AI spawns a new generation of job roles

David also highlighted that -- now more than ever -- leaders need to provide a steady, "non-anxious presence" to reassure people that it will be OK through this transition, even if the outcomes remain uncertain. This means openly acknowledging people's fears, showing genuine empathy, communicating transparently, and co-creating solutions.

Together, the speakers emphasized that responsible and ethical AI adoption requires empathetic change management and responsible governance frameworks. Leaders should promote psychological safety through transparency, reskilling support, reassurance during uncertain transitions, and co-designing solutions tailored to people's needs.

Deployment empathy also includes recognizing the importance of AI adoption and managing unintended consequences that requires cross-sector collaboration between government, academia, civil society groups, and business. We need new social contracts for labor displacement and other seismic economic shifts catalyzed by AI.

Also: AI is changing cybersecurity and businesses must wake up to the threat

Cumulatively, the speakers highlighted the societal leadership challenges posed by AI and that leaders have a duty to support their workforce through AI adoption with empathy, communication, and responsible governance. Leaders must champion deployment empathy both internally and externally to their organizations. Together with radical collaboration, clear governance guardrails, and compassionate communication, leaders can guide their organizations through the AI-driven transformation in a productive way.

This article was co-authored by Dr. David Bray, Principal & CEO at LeadDoAdapt (LDA) Ventures.

/ artificial intelligence

Your board needs no-nonsense AI leadership - these experts explain why

Policymakers, business leaders, and technology experts all agree on the need for a pragmatic, inclusive, and responsible approach to AI. How do we get there?

Written by **Vala Afshar,** Contributing Writer

Aug. 7, 2024 at 3:00 a.m. PT

AzmanL/Getty Images

IDC estimates that companies invested $16B in generative AI solutions in 2023, and that they'll invest $140B in 2027 -- a compound annual growth rate (CAGR) of 70%, according to the Trends in AI for CRM research from Salesforce. Whether generating content and communications or optimizing processes, teams are discovering the best ways to incorporate AI in the flow of their work as investments ramp up.

No fewer than 92% of sales, service, marketing, or commerce teams are at least considering AI investments. AI is the top priority for CEOs and -- quite often -- a high-priority discussion in the boardroom. And that discussion goes beyond technology, encompassing the workplace skills and policies needed in the AI era.

Also: AI can mean big business benefits. But these obstacles must be cleared first

Employees recognize the transformative impact of AI on their careers, but their employers are largely falling behind in empowering them for success. Fifty-six percent of desk workers believe generative AI will transform their roles, but only 21% say their company has provided clear policies around its use.

To better understand the nature of AI discussions and priorities in the boardroom, DisrupTV weekly podcast -- co-hosted by Constellation Research CEO and founder Ray Wang and yours truly -- dove into the crucial role of responsible AI governance in a rapidly evolving technological landscape.

Our discussion featured three prominent executives from the public and private sector with senior leadership and boardroom experience: Miriam Vogel, president and CEO of Equal AI, a non-profit dedicated to promoting responsible AI governance; Teresa Carlson, a venture capitalist with General Catalyst and a private sector investor with extensive experience in technology and government; and Dr. David Bray, a champion of positive change and a leading voice on technology's impact on governments and businesses alike with the non-partisan Stimson Center.

Miriam Vogel's insights

Miriam Vogel, a leading voice in responsible AI governance, underscored the importance of inclusivity and equity in AI development and deployment. She emphasized the need to ensure that AI benefits all communities, not just a select few. She advocated for AI literacy, urging individuals to understand the capabilities and limitations of AI tools. Vogel also highlighted the importance of engaging diverse populations in AI development, ensuring that AI systems are representative of the communities they serve.

Also: Can AI even be open source? It's complicated

Vogel emphasized the need for a global consensus on AI definitions and standards, particularly in the absence of clear international frameworks. She stressed the importance of industry, government, and society working together to establish best practices for responsible AI governance. She highlighted the work of Equal AI in promoting responsible AI governance through programs for business leaders, policymakers, and lawyers.

Teresa Carlson's vision

Teresa Carlson shared her perspective on the exciting opportunities and challenges presented by generative AI. She emphasized the need for a risk-based approach to AI, acknowledging the potential for cybersecurity threats. Carlson highlighted the rapid pace of technological innovation and the need for technologies that can keep pace with evolving threats.

Also: These experts believe AI can help us win the cybersecurity battle

Carlson emphasized the importance of global resilience in the face of geopolitical shifts and the increasing focus on national technological sovereignty. She highlighted the growing investment in AI across various sectors, including defense, healthcare, and legal. She emphasized the need for companies to move fast and responsibly, taking advantage of the opportunities presented by AI while ensuring ethical and inclusive development.

David Bray's perspective

Dr. Bray emphasized the need for a pragmatic approach to AI, urging companies and governments to prioritize the business case before deploying AI technology. He highlighted the risks that organizations face when adopting AI without fully understanding its implications, potentially leading to unintended consequences.

He stressed the importance of respecting data and recognizing the diverse needs of different communities, particularly in free and open societies like the US and similar nations. Dr. Bray also warned of the potential for AI to be misused for malicious purposes, such as creating misinformation at an unprecedented scale. He advocated for private-sector solutions to counter these threats, emphasizing the need for tools that help people discern accurate information from fabricated content. He highlighted the importance of data governance and the need to move beyond the outdated "data is the new oil" metaphor, suggesting a shift toward data cooperatives and communities.

1:04:51

The importance of collaboration: Our podcast underscored the importance of collaboration among industry, government, and non-profit organizations in shaping the future of AI. The panelists emphasized the need for a multi-stakeholder approach to address the challenges and opportunities presented by AI. They highlight the importance of public-private partnerships, government funding, and venture capital investment in driving responsible AI innovation.

The future of AI: In summarizing the DisrupTV episode, we observed similar themes in the predictions presented for the future of AI. Each of our three guests emphasized the need for continued education and training to prepare the workforce for a world increasingly shaped by AI. They highlighted the importance of AI literacy, particularly for younger generations, to ensure that AI is used responsibly and effectively. The guests also emphasized the need for a more inclusive approach to AI development, ensuring that all communities benefit from its advancements.

Also: How to run dozens of AI models on your Mac or PC - no third-party cloud needed

Key takeaways: Vogel, Carlson, and Bray provided valuable insights for the strategic boards of businesses and government alike regarding the critical issues surrounding AI governance and its impact on society. They agreed on the need for a pragmatic, inclusive, and responsible approach to AI, ensuring that its benefits are shared by all. They also all agreed on the importance of collaboration, education, and investment in shaping a future where AI serves as a force for good.

This article was co-authored by Dr. David Bray, principal and CEO at LeadDoAdapt (LDA) Ventures.

/ artificial intelligence

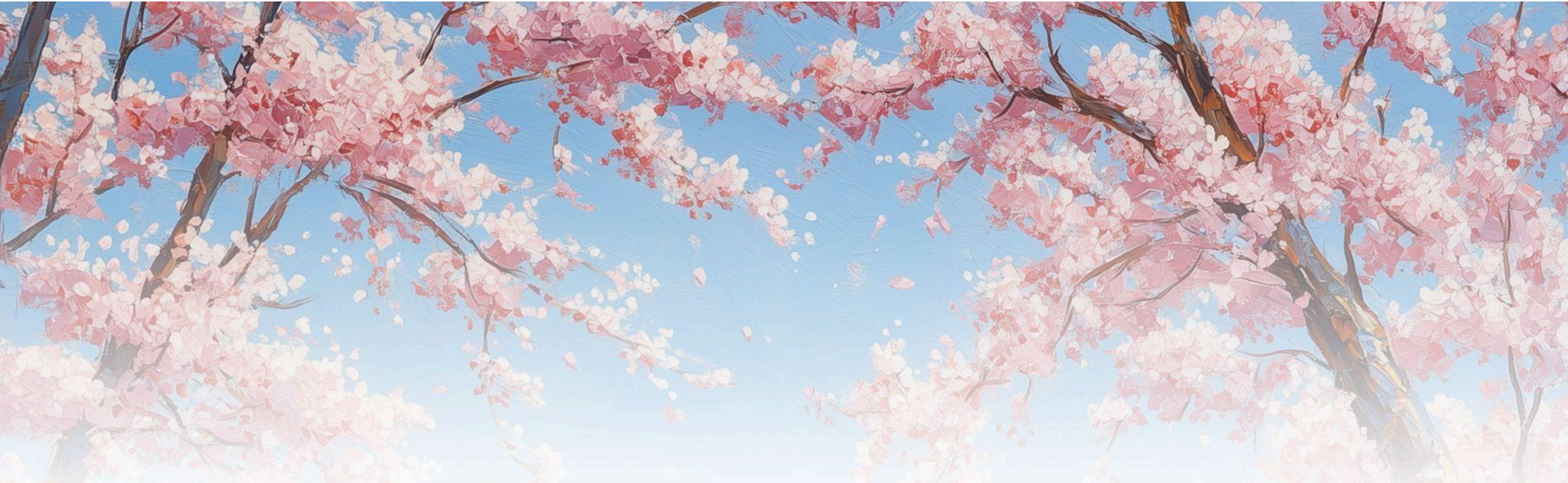
U.S. HEALTHCARE THAT WORKS

TRANSFORMATION THROUGH MARKET-DRIVEN INNOVATION

A REPORT BY GENERAL CATALYST INSTITUTE

MARCH 2025

INDEX



FOREWORD

Healthcare in America stands at a crossroads: embrace transformation or protect the status quo. After decades of fragmentation, rising costs, and uneven outcomes, we're witnessing an unprecedented opportunity to fundamentally reshape the industry through market-driven solutions - powered by applied AI.

General Catalyst has been at the forefront of healthcare innovation, investing in companies that are not merely incrementally improving the system but reimagining it entirely. At the General Catalyst Institute (GCI) a key part of our role is to educate policymakers on the most cutting-edge health tech solutions to help shape effective public policy.

And that's the point of this report. In it, we discuss priority issue areas ripe for modernization and the need to remove policy blockers that impede the ability to deliver high quality value-based care. Within our Catalyzing Care: A Framework for a Healthier America we outline five key pillars to help transform U.S. healthcare delivery:

1. Foster Healthier Outcomes for All
2. Refine Needed Innovations Without Red Tape
3. Advance Patient-First Care, Data and Accessibility
4. Maximize Fiscal Responsibility for U.S. Healthcare
5. Enhance U.S. Medical Talent for Today and Tomorrow

Each of these pillars has an associated short-term and long-term policy recommendation. If implemented, the impact for real people would be remarkable: Doctors could save thousands more lives each year and patients in rural and underserved communities could connect with specialists regardless of their location through care networks enhanced by AI, preventing hundreds of thousands of unnecessary hospitalizations.

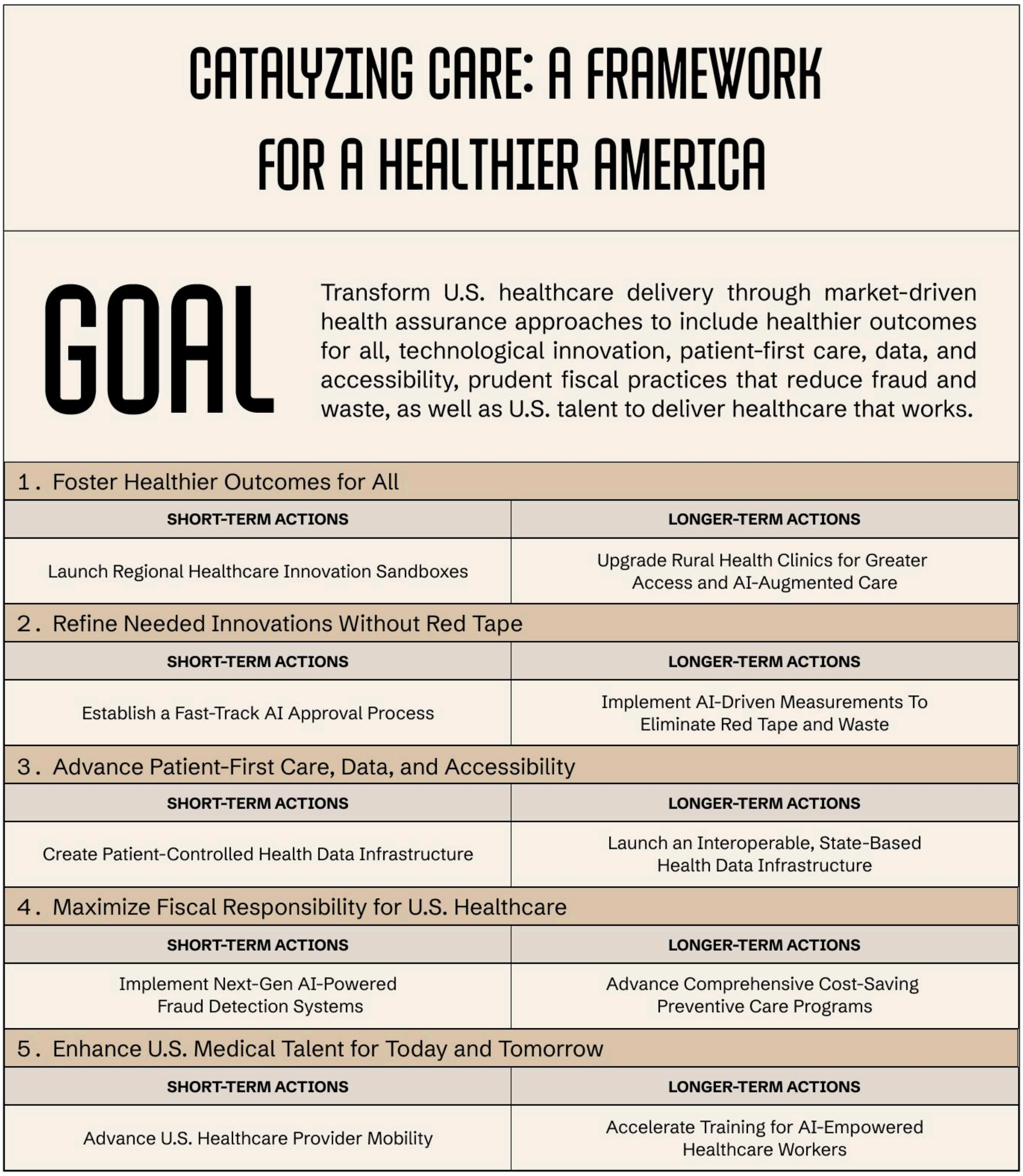
Throughout my career in both public and private sectors, I've witnessed firsthand that our nation is at its most innovative and effective when private sector partners unite around a shared vision of national impact. Repeatedly, I've seen how market-driven solutions, coupled with purposeful collaboration, can solve our most pressing challenges. This moment in healthcare is no different – in fact, it may be one of our greatest opportunities yet.

The time for transformative action is now. Whether you're a healthcare provider, technology innovator, policymaker, or educational organization, your participation in this effort can help shape a healthcare system that truly delivers for all. By striving for transformative actions, it is also imperative to utilize these technologies in order to cut away the fraud and wasteful spending in the U.S. healthcare system. Together, let's build the future healthcare system we want and deserve for all Americans.

Sincerely,

Teresa H. Carlson

Teresa Carlson
Founding President
General Catalyst Institute



CATALYZING CARE: A FRAMEWORK FOR A HEALTHIER AMERICA

GOAL Transform U.S. healthcare delivery through market-driven health assurance approaches to include healthier outcomes for all, technological innovation, patient-first care, data, and accessibility, prudent fiscal practices that reduce fraud and waste, as well as U.S. talent to deliver healthcare that works.

1. Foster Healthier Outcomes for All

SHORT-TERM ACTIONS	LONGER-TERM ACTIONS
Launch Regional Healthcare Innovation Sandboxes	Upgrade Rural Health Clinics for Greater Access and AI-Augmented Care

2. Refine Needed Innovations Without Red Tape

SHORT-TERM ACTIONS	LONGER-TERM ACTIONS
Establish a Fast-Track AI Approval Process	Implement AI-Driven Measurements To Eliminate Red Tape and Waste

3. Advance Patient-First Care, Data, and Accessibility

SHORT-TERM ACTIONS	LONGER-TERM ACTIONS
Create Patient-Controlled Health Data Infrastructure	Launch an Interoperable, State-Based Health Data Infrastructure

4. Maximize Fiscal Responsibility for U.S. Healthcare

SHORT-TERM ACTIONS	LONGER-TERM ACTIONS
Implement Next-Gen AI-Powered Fraud Detection Systems	Advance Comprehensive Cost-Saving Preventive Care Programs

5. Enhance U.S. Medical Talent for Today and Tomorrow

SHORT-TERM ACTIONS	LONGER-TERM ACTIONS
Advance U.S. Healthcare Provider Mobility	Accelerate Training for AI-Empowered Healthcare Workers

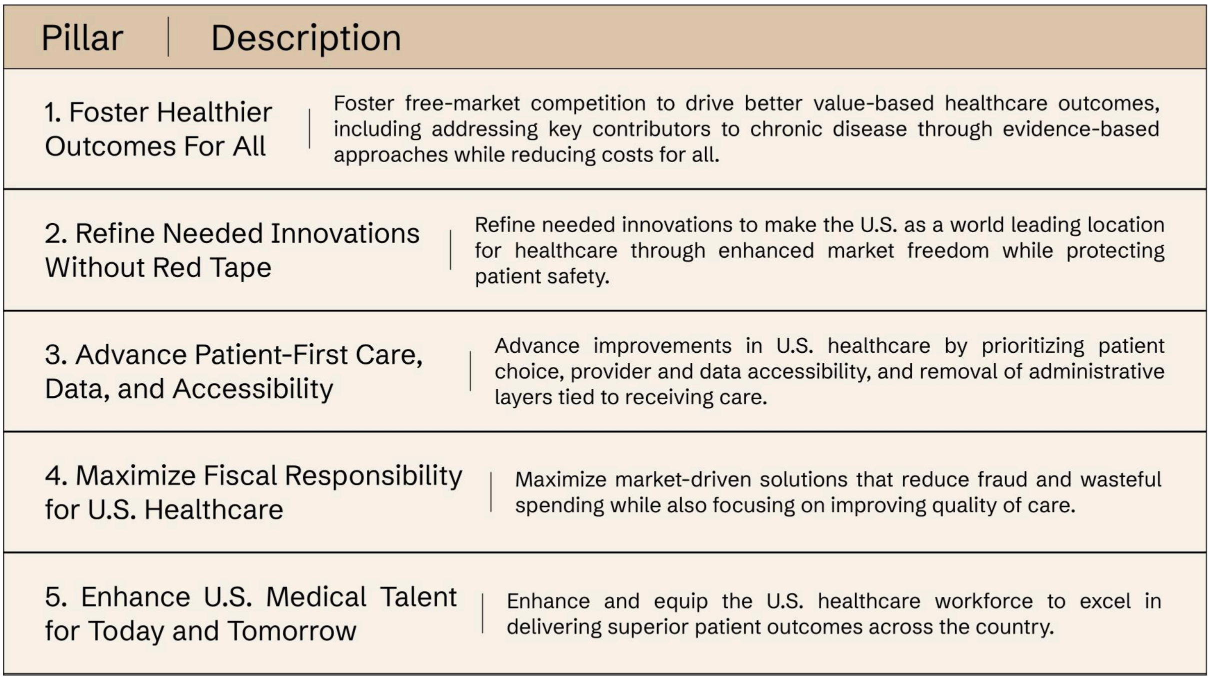
Figure 1: Catalyzing Care: A Framework for a Healthier America - Goal, Pillars, & Actions

CALL TO ACTION

The time for transformative action in U.S. healthcare is now. Leading companies, innovative startups, and forward-thinking organizations across America can unite in their vision to produce U.S. healthcare that works through market-driven approaches that leverage innovative technologies while prioritizing value-based health care outcomes, privacy, and patient safety through 'radical transparency' in healthcare delivery systems.

Together we will transform U.S. healthcare delivery through market-driven health assurance approaches to include healthier outcomes for all, technological innovation, patient-first care, data, and accessibility, prudent fiscal practices that reduce fraud and waste, and U.S. talent to deliver healthcare that works.

CATALYZING CARE: A FRAMEWORK FOR A HEALTHIER AMERICA



Pillar	Description
1. Foster Healthier Outcomes For All	Foster free-market competition to drive better value-based healthcare outcomes, including addressing key contributors to chronic disease through evidence-based approaches while reducing costs for all.
2. Refine Needed Innovations Without Red Tape	Refine needed innovations to make the U.S. as a world leading location for healthcare through enhanced market freedom while protecting patient safety.
3. Advance Patient-First Care, Data, and Accessibility	Advance improvements in U.S. healthcare by prioritizing patient choice, provider and data accessibility, and removal of administrative layers tied to receiving care.
4. Maximize Fiscal Responsibility for U.S. Healthcare	Maximize market-driven solutions that reduce fraud and wasteful spending while also focusing on improving quality of care.
5. Enhance U.S. Medical Talent for Today and Tomorrow	Enhance and equip the U.S. healthcare workforce to excel in delivering superior patient outcomes across the country.

Figure 2: Catalyzing Care Framework Pillars

United by the five pillars for Catalyzing Care: A Framework for a Healthier America, the launch of this paper represents a rallying call to deliver U.S. healthcare that works. This includes companies focused on automating healthcare interactions, companies building rural health systems, companies working on Medicaid solutions, companies delivering better health outcomes daily, and companies pioneering solutions dedicated to preventive care, workforce transformation, and technological innovation. This rallying call also includes those collaborating with major partners to deploy AI tools in healthcare systems, while also working with U.S. policymakers, Congressional leaders, and State leaders to create practical solutions for healthcare challenges. This also includes organizations helping with community health worker programs, both state and rural healthcare initiatives, as well as innovative payment systems – working to make healthcare more proactive, affordable, and accessible.

Specifically, the **Catalyzing Care: A Framework for a Healthier America** centers around five pillars that set the foundation to transform U.S. healthcare delivery through market-driven health assurance approaches:

1. Foster Healthier Outcomes for All
Fostering free-market competition to drive better value-based healthcare outcomes, including addressing key contributors to chronic disease through evidence-based approaches while reducing costs for all. Across thousands of rural and urban clinics nationwide, healthcare providers could deploy AI-driven patient engagement and monitoring tools to proactively identify and support millions of high-risk patients with chronic conditions like diabetes, creating a scalable model for value-based care that demonstrably improves health outcomes while reducing costs through early intervention and personalized care delivery.

2. Refine Needed Innovations Without Red Tape
Refining needed innovations to make the U.S. as a world leading location for healthcare through enhanced market freedom while protecting patient safety. Thousands of hospital systems nationwide could implement and rapidly validate AI-powered sepsis detection tools that analyze near real-time patient vitals to identify warning signs hours earlier than traditional methods, potentially saving tens of thousands of lives annually while reducing ICU admissions and healthcare costs through a streamlined regulatory pathway that enables swift deployment and reimbursement based on demonstrated outcomes.

3. Advance U.S. Patient-First Care, Data, and Accessibility
Advancing improvements to U.S. healthcare by prioritizing patient choice, provider accessibility, and removal of administrative layers tied to receiving care. Patients managing complex conditions like cancer could securely share their complete medical histories through AI-powered platforms that seamlessly connect all their healthcare providers nationwide, eliminating billions

in redundant tests while ensuring near real-time care coordination and data-driven personalization, ultimately delivering better health outcomes and improved experiences for patients while reducing healthcare costs in parallel to reducing fraud and wasteful spending across the entire system.

4. Maximize Fiscal Responsibility for U.S. Healthcare
Maximizing market-driven solutions that reduce fraud and wasteful spending while also focusing on improving quality of care. Next-generation AI paired with the right datasets could rapidly flag anomalies, such as a provider suddenly billing excessive high-cost procedures, before payments are issued, preventing billions in losses. Replacing the outdated "pay-and-chase" model with near real-time fraud detection would protect taxpayer dollars, strengthen program integrity, and ensure faster, accurate payments for legitimate health providers.

5. Enhance U.S. Medical Talent for Today and Tomorrow
Enhance and equip the U.S. healthcare workforce to excel in delivering superior patient outcomes across the country. Hundreds of thousands of qualified U.S. healthcare providers could deliver care across state lines, especially benefiting rural communities to access health specialists previously out of reach while reducing the administrative costs by millions through automated verification systems. This approach also would create an interoperable framework for reducing fraudulent license registrations or fraudulent claims through such a system.

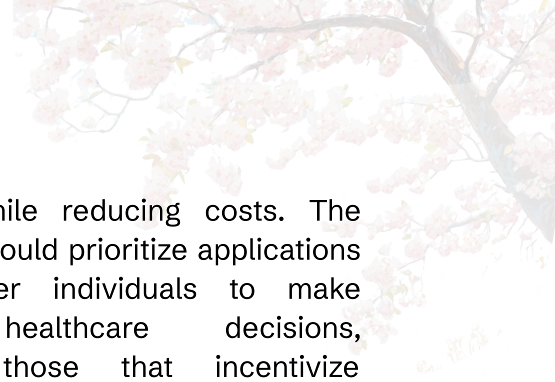
Building on these pillars, the following short-term and long-term actions represent a clear pathway to making U.S. healthcare the best in the world, combining the strengths of both the public and private sector to create lasting, positive change.

SHORT-TERM ACTIONS

Achievable Within 9 Months

Launch Regional Healthcare Innovation Sandboxes

In the immediate short-term, The Department of Health and Human Services (HHS) can establish designated geographic regions as healthcare innovation sandboxes through existing waiver authorities, creating controlled environments where healthcare providers and technology companies can test innovative care delivery models. These sandboxes would operate under streamlined regulatory frameworks while maintaining essential safety standards, allowing for rapid deployment and evaluation of innovative approaches to healthcare delivery. Value-based care comes in many forms, including quality bonus payments with limited financial alignment, and success depends on risk sharing tied to health outcomes. These sandboxes would help bridge toward true outcomes-based care by allowing companies to test patient engagement tools that drive measurable improvements in health outcomes while lowering costs. The initiative would prioritize regions with diverse demographic and socioeconomic populations to ensure comprehensive testing of new



healthcare models. Healthcare providers within these sandboxes would have the flexibility to implement artificial intelligence (AI)-driven solutions across various aspects of care delivery, from patient scheduling to treatment planning and care coordination. Regular evaluation periods would assess effectiveness, guiding broader implementation.

State governments would collaborate with local healthcare systems and private sector technology providers to establish clear metrics for success, focusing on measurable improvements in patient outcomes, cost reduction, and accessibility of care. These partnerships would facilitate data sharing and analysis while maintaining patient privacy and security standards. The metrics would encompass both quantitative measures such as treatment outcomes and cost savings, and qualitative assessments of patient and provider satisfaction. These sandboxes will support the 'Make America Healthy Again' movement by testing interventions that address root causes of chronic disease, including environmental factors and food additives, while maintaining rigorous scientific standards.

In addition, HHS, CMS, and FDA should jointly establish strategic innovation sandboxes in key geographic regions that specifically focus on consumer-facing healthcare applications tied to value-based care outcomes. These sandboxes will serve as proving grounds where innovative companies can test new patient engagement tools and value-based care solutions without navigating unnecessary regulatory barriers, with special emphasis on applications that demonstrate measurable improvements in health outcomes while reducing costs. The sandboxes should prioritize applications that empower individuals to make informed healthcare decisions, particularly those that incentivize preventive care and healthy choices through market-based approaches. Special emphasis should be placed on solutions that can demonstrate measurable improvements in health outcomes while reducing costs, with successful innovations being fast-tracked for broader implementation. This approach will particularly benefit rural and underserved communities by testing new models of care delivery that overcome traditional access barriers while promoting value-based care principles.

Federal and state agencies would work together to create streamlined approval processes for sandbox participants while establishing clear accountability measures that protect patient safety and

ACTION IN SUM

Across thousands of rural and urban clinics nationwide, healthcare providers could deploy AI-driven patient engagement and monitoring tools to proactively identify and support millions of high-risk patients with chronic conditions like diabetes, creating a scalable model for value-based care that demonstrably improves health outcomes while reducing costs through early intervention and personalized care delivery.

This action would streamline approval processes for healthcare innovation sandbox participants while establishing clear accountability measures. This initiative primarily supports Pillars 1 and 2, catalyzing free-market competition, while advancing innovation and demonstrates how reduced regulatory barriers can accelerate healthcare transformation.

privacy. This collaborative approach would include standardized templates across HHS, CMS, and FDA efforts for reporting and evaluation to reduce administrative burden on participants. A dedicated support team would be established to help participants navigate regulatory requirements and share best practices in healthcare delivery. The initiative would include a formal process for scaling successful innovations beyond the sandbox regions.

Establish a Fast-Track AI Approval Process

The FDA can create an expedited pathway for reviewing and approving AI-driven healthcare solutions that demonstrate clear potential for improving patient outcomes while maintaining rigorous safety standards. This process would leverage existing regulatory frameworks while introducing new mechanisms specifically designed for AI applications in healthcare. As top priority, HHS immediately should charge the Office of the National Coordinator/Assistant Secretary for Technology Policy's (ONC/ASTP) to evaluate existing HTI-1 rules and do more to eliminate anti-competitive barriers for innovative AI companies. This would prevent electronic health record (EHR) vendors from blocking or stealing innovations from emerging companies. The pathway would include continuous monitoring protocols that allow for near real-time assessment of AI performance and safety in clinical settings, enabling rapid response to any emerging concerns while facilitating quick adoption of beneficial updates.

Private sector companies would work in close partnership with FDA to establish clear, measurable criteria for fast-track eligibility, focusing on solutions that address critical healthcare needs or demonstrate significant improvements over existing approaches. These criteria would include specific metrics for measuring AI performance, safety parameters, and potential impact on patient outcomes. The process would incorporate feedback loops from healthcare providers and patients to ensure real-world effectiveness and usability of approved AI solutions.

The fast-track process should include a two-tier AI reimbursement pathway to include Phase 1: Allow AI tools to be deployed in real-world settings under clear Quality Management System standards and Phase 2 : Upon demonstrating positive patient outcomes and cost savings, these tools become eligible for full reimbursement. The implementation would include robust post-market monitoring systems that leverage AI itself to monitor the performance and safety of approved solutions in real-world settings. This would enable rapid identification and response to any safety concerns while providing valuable data for continuous improvement. The program would establish clear protocols for updating and modifying approved AI solutions to reflect new learning and capabilities, ensuring that approved solutions can evolve while maintaining safety standards.

Tied to establishing a fast-track AI approval process, HHS should immediately transfer the authority for monitoring and enforcing anti-competitive practices in healthcare technology, to include AI in healthcare, from HHS Inspector Generals to the ONC. This shift will enable more proactive and specialized oversight of anti-competitive behaviors, particularly in the health information technology (IT) and AI sectors. ONC's deep technical expertise and understanding of the healthcare technology ecosystem makes it better positioned to identify and address anti-competitive practices before they harm innovation or patient outcomes. By consolidating this authority under ONC, HHS can create a more streamlined and effective enforcement mechanism that prevents incumbent vendors from blocking or stealing innovations from emerging companies. This change will help ensure that innovative healthcare solutions, including AI in healthcare, can reach markets more quickly while maintaining appropriate safety and privacy standards.

ACTION IN SUM

Thousands of hospital systems nationwide could implement and rapidly validate AI-powered sepsis detection tools that analyze real-time patient vitals to identify warning signs hours earlier than traditional methods, potentially saving tens of thousands of lives annually while reducing ICU admissions and healthcare costs through a streamlined regulatory pathway that enables swift deployment and reimbursement based on demonstrated outcomes.

This action would create an expedited pathway for reviewing and approving AI-driven healthcare solutions while maintaining rigorous safety standards through continuous monitoring. This initiative primarily supports Pillar 2, advancing needed innovations without red tape, while also contributing to Pillar 1 by accelerating the deployment of beneficial healthcare technologies.

Create Patient-Controlled Health Data Infrastructure

As part of this health data infrastructure, CMS should establish a secure, standardized "Innovation Data Commons" consisting of its own internal data that makes de-identified healthcare data available to qualified U.S. companies developing AI solutions for healthcare improvement. This platform would leverage HL7 standards and modern API architectures to enable secure and responsible access to CMS's data resources while maintaining robust privacy protections. By creating clear accountability frameworks and market-driven access protocols, CMS can unleash private sector innovation while ensuring appropriate use of sensitive health information.

Private sector companies would participate in the commons to build tech-enabled services on top of the data that empowers patients with agency with regards to their health outcomes and clinicians with better ways to work with patients to improve value-based delivery of care. This patient-centric approach would eliminate data silos that currently fragment CMS healthcare delivery, enabling seamless coordination between providers while maintaining individual privacy rights. HL7's Fast Healthcare Interoperability Resources (FHIR) standards should serve as the foundation for this infrastructure, ensuring vendor-neutral data exchange and enabling seamless integration across different healthcare systems while maintaining patient control. To further promote competition and innovation, HHS should repeal HTI-1 rules, which currently enable incumbent EHR vendors to block AI solutions that could improve care.

Furthermore, this infrastructure would serve as a catalyst for U.S. healthcare innovation by creating a standardized, interoperable foundation upon which new healthcare solutions can be built beyond CMS's own data. By establishing clear data governance frameworks and market-driven access protocols, the system would enable qualified healthcare companies to develop AI-powered tools and services that improve patient outcomes while maintaining strict privacy protections. This approach would accelerate the development of personalized medicine, predictive analytics, and other advanced healthcare technologies while ensuring that patients maintain ultimate control over their health information. This approach also would aid in using next-generation AI solutions to assist with near real-time identification of fraud and wasteful spending on healthcare. The system would also include robust audit trails and transparency mechanisms, allowing patients to see exactly how their data is being used while holding healthcare organizations accountable for maintaining data privacy and security standards.

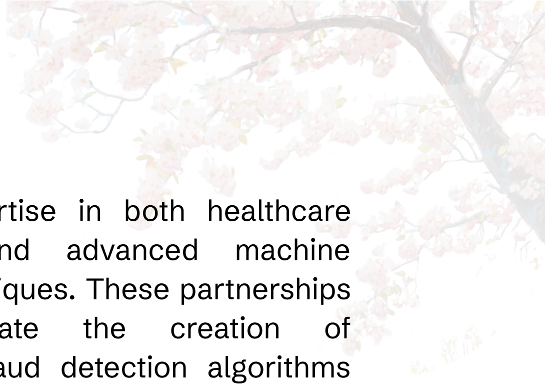
Companies would be evaluated based on their potential to improve health outcomes and reduce costs, with successful innovations being fast-tracked for broader implementation. This approach would help position the U.S. as a stronger leader in AI-enabled healthcare innovation while creating a competitive marketplace that drives better patient outcomes. This Innovation Data Commons would specifically prohibit anti-competitive data access arrangements, thereby ensuring that both established companies and innovative startups have equal opportunity to leverage CMS data for developing breakthrough healthcare solutions. This market-driven approach to data access would accelerate the development of AI tools that can improve care quality, reduce costs, and advance the overall U.S. healthcare system.

HHS, CMS, and FDA should actively partner with state attorneys general (AGs) to leverage the existing authorities of the 21st Century CURES Act to prosecute anti-competitive practices impeding market-based solutions including healthcare technology and data sharing to advance better health outcomes. This collaboration should particularly focus on vendors who create artificial data silos or block innovative AI solutions that could improve patient outcomes. The agencies should provide technical expertise and evidence to support State AGs in pursuing cases against EHR vendors and other healthcare technology companies that engage in anti-competitive behaviors, such as blocking data access or requiring innovative companies to

ACTION IN SUM

Patients managing complex conditions like cancer could securely share their complete medical histories through AI-powered platforms that seamlessly connect all their healthcare providers nationwide, eliminating billions in redundant tests while ensuring near real-time care coordination and data-driven personalization, ultimately delivering better health outcomes and improved experiences for patients while reducing healthcare costs in parallel to reducing fraud and wasteful spending across the entire system.

This action would establish a secure, patient-controlled data infrastructure that empowers individuals to manage their health information, while enabling efficient care coordination. This initiative primarily supports Pillar 3, revolutionizing patient-first care, while also contributing to Pillar 1 by catalyzing much-needed innovation in healthcare services.



share their intellectual property as a condition of market access. This enforcement strategy should emphasize the CURES Act's original intent to promote interoperability and prevent information blocking, while ensuring that health data can be responsibly used to develop and deploy AI solutions that improve care quality and reduce costs. By working with State AGs, federal agencies can create a more competitive marketplace that encourages innovation while protecting patient interests.

Implement Next-Gen AI-Powered Fraud Detection Systems

CMS can deploy a comprehensive, state-of-the-art AI solution that leverages machine learning algorithms to identify and prevent healthcare fraud in near real-time, focusing initially on high-risk areas within Medicare and Medicaid programs. The system would utilize advanced pattern recognition to analyze claims data across multiple dimensions, including provider behavior, patient utilization patterns, and billing anomalies, while maintaining patient privacy and data security standards. This implementation would include near real-time monitoring capabilities that can flag suspicious activities before payments are processed, significantly reducing the current pay-and-chase model of fraud prevention. The system would also incorporate natural language processing to analyze unstructured data from medical records and clinical provider notes, providing a more complete picture of potentially fraudulent activities. Additionally, the system would be designed with adaptive learning capabilities to stay ahead of emerging fraud schemes and patterns.

Private sector technology partners would collaborate closely with CMS to develop and refine these AI models, bringing expertise in both healthcare operations and advanced machine learning techniques. These partnerships would facilitate the creation of specialized fraud detection algorithms that can identify subtle patterns and relationships within vast amounts of healthcare data. The private sector would also contribute expertise in data security and privacy protection, ensuring that the system meets all regulatory requirements while maintaining operational efficiency. State-level Medicaid programs would provide valuable input on local fraud patterns and challenges, helping to create more targeted and effective detection mechanisms.

The implementation would include a robust feedback loop system where successful fraud identifications are used to continuously improve the AI models' accuracy and effectiveness. Regular performance assessments would measure both the system's ability to detect fraud and its impact on legitimate claims processing, ensuring that proper healthcare delivery is not impeded. The program would establish clear protocols for investigating AI-flagged cases, including mechanisms for providers to quickly resolve false positives. This initiative would serve as a model for broader implementation of AI-driven solutions in healthcare administration, demonstrating how technology can improve system efficiency while protecting public resources.

HHS, CMS, and FDA should actively partner with state attorneys general (AGs) to leverage the existing authorities of the 21st Century CURES Act to prosecute anti-competitive practices impeding market-based solutions including healthcare technology and data sharing to advance better health outcomes. This collaboration should particularly focus on vendors who create artificial data silos or block innovative AI solutions that could improve patient outcomes. The agencies should provide technical expertise and evidence to support State AGs in pursuing cases against EHR vendors and other healthcare technology companies that engage in anti-competitive behaviors, such as blocking data access or requiring innovative companies to share their intellectual property as a condition of market access. This enforcement strategy should emphasize the CURES Act's original intent to promote interoperability and prevent information blocking, while ensuring that health data can be responsibly used to develop and deploy AI solutions that improve care quality and reduce costs. By working with State AGs, federal agencies can create a more competitive marketplace that encourages innovation while protecting patient interests.

ACTION IN SUM

In 2024, Medicare Fee-for-Service saw $31.7 billion and Medicaid $31.1 billion in improper payments, much of it due to billing errors and potential fraud as reported by CMS in 2025. Next-generation AI paired with the right datasets could rapidly flag anomalies, such as a provider suddenly billing excessive high-cost procedures, before payments are issued, preventing billions in losses. Replacing the outdated "pay-and-chase" model with near real-time fraud detection would protect taxpayer dollars, strengthen program integrity, and ensure faster, accurate payments for legitimate health providers.

This action would implement next-generation AI-powered systems for near real-time fraud detection and prevention in Medicare and Medicaid programs, significantly reducing improper payments through advanced pattern recognition. This initiative directly addresses Pillar 4, expediting fiscal responsibility while also advancing Pillar 2, advancing needed innovations without red tape, by demonstrating how technology can improve healthcare system efficiency.

Advance U.S. Healthcare Provider Mobility

HHS, CMS, and FDA should establish a groundbreaking 'Make America Healthy Again' Credentials Program that revolutionizes how healthcare providers practice across state lines. This voluntary federal licensure framework would enable providers already credentialed in one state, for example with CMS, to deliver care throughout all U.S. states and territories, dramatically expanding access to quality healthcare. By leveraging existing federal authorities, this initiative would create a streamlined pathway for qualified providers to serve both federal health program beneficiaries and, through strategic partnerships, private insurance patients across state boundaries.

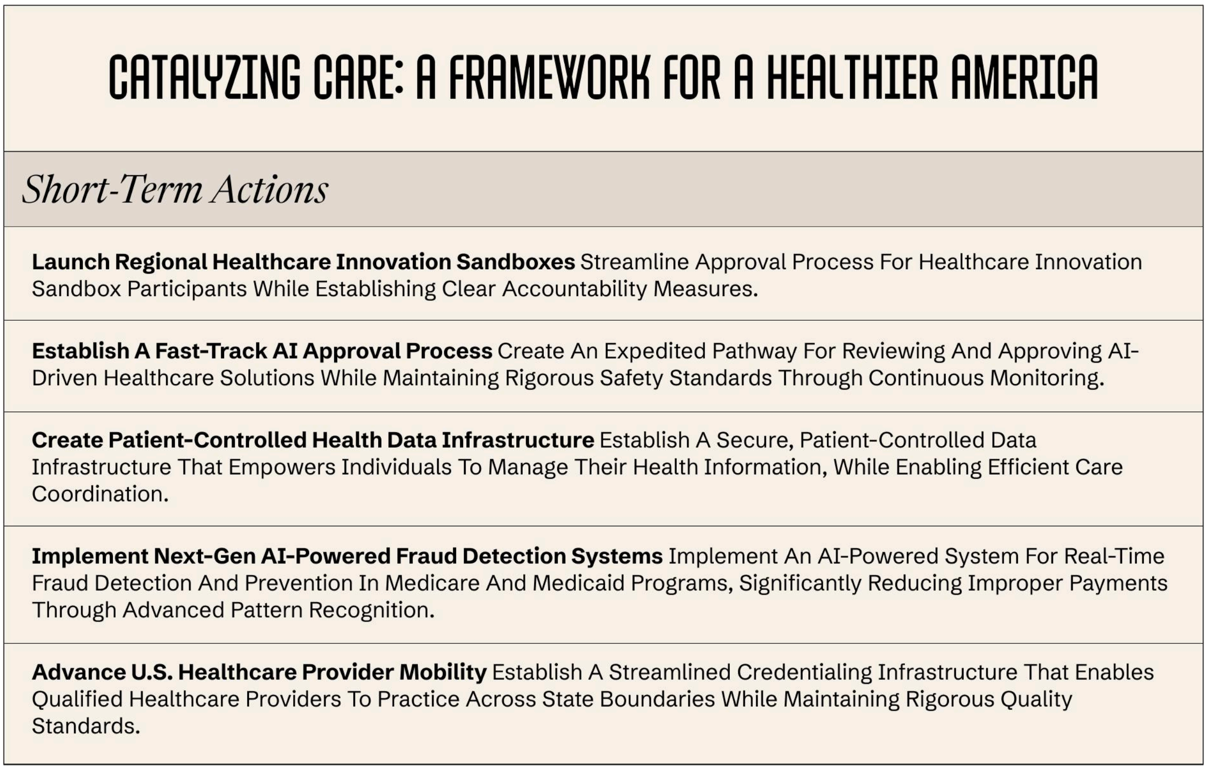
The program would implement next-generation verification systems for interoperable credentials across different states, thereby enabling rapid provider onboarding of healthcare workers, while reducing fraudulent license registrations or fraudulent claims through such a system. This technology-driven approach also would significantly reduce administrative burden and costs associated with multi-state licensure, while ensuring comprehensive verification of provider qualifications and practice history. The system would incorporate continuous monitoring of provider performance metrics and patient outcomes, creating an interoperable data-driven framework for maintaining high-quality care standards across state lines. This would be particularly valuable for telehealth services and specialized care delivery, where geographic barriers have traditionally limited access to expertise.

This reform would be transformative for rural and underserved communities that currently face significant healthcare access challenges. By enabling qualified providers to practice across state lines more easily, these communities would gain access to a broader pool of healthcare professionals and specialists. This comprehensive approach would help address critical healthcare workforce shortages while promoting the adoption of innovative care delivery models that can improve outcomes and reduce costs.

ACTION IN SUM

Hundreds of thousands of qualified U.S. healthcare providers could deliver care across state lines, especially benefiting rural communities to access health specialists previously out of reach while reducing the administrative costs by millions through automated verification systems. This approach also would create an interoperable framework for reducing fraudulent license registrations or fraudulent claims through such a system.

This action would establish a streamlined credentialing infrastructure that enables qualified healthcare providers to practice across state boundaries while maintaining rigorous quality standards. This initiative primarily supports Pillar 5, strengthening U.S. medical talent, while also contributing to Pillar 3 by enabling more effective use of healthcare technology.



CATALYZING CARE: A FRAMEWORK FOR A HEALTHIER AMERICA

Short-Term Actions

Launch Regional Healthcare Innovation Sandboxes Streamline Approval Process For Healthcare Innovation Sandbox Participants While Establishing Clear Accountability Measures.

Establish A Fast-Track AI Approval Process Create An Expedited Pathway For Reviewing And Approving AI-Driven Healthcare Solutions While Maintaining Rigorous Safety Standards Through Continuous Monitoring.

Create Patient-Controlled Health Data Infrastructure Establish A Secure, Patient-Controlled Data Infrastructure That Empowers Individuals To Manage Their Health Information, While Enabling Efficient Care Coordination.

Implement Next-Gen AI-Powered Fraud Detection Systems Implement An AI-Powered System For Real-Time Fraud Detection And Prevention In Medicare And Medicaid Programs, Significantly Reducing Improper Payments Through Advanced Pattern Recognition.

Advance U.S. Healthcare Provider Mobility Establish A Streamlined Credentialing Infrastructure That Enables Qualified Healthcare Providers To Practice Across State Boundaries While Maintaining Rigorous Quality Standards.

Figure 3. Short-Term Actions

LONGER-TERM ACTIONS

Achievable Within 2 Years

Upgrade Rural Health Clinics for Greater Access and AI-Augmented Care

Over the longer-term, to truly transform U.S. healthcare delivery through market-driven health assurance, HHS, CMS, and FDA can modernize existing Federally Qualified Health Centers (FQHCs) through AI-enabled care delivery models. Building upon FQHCs, the U.S. can create a network of AI-powered rural health hubs that combine telehealth infrastructure, mobile health units, and community health workers to deliver cost-effective care to underserved rural communities. This comprehensive initiative would leverage the "Health Assurance Line" concept mentioned in the knowledge source, expanding it to include physical infrastructure and AI-enabled diagnostic capabilities in rural areas. The system would utilize advanced predictive analytics to optimize resource allocation, ensuring that mobile health units and specialists are deployed to areas with the greatest need at the most critical times. The program would also incorporate innovative payment models that incentivize preventive care and healthy choices while reducing costs through efficient resource utilization and early intervention strategies.

Private sector partners would collaborate to develop and implement AI-powered solutions specifically designed for rural healthcare challenges. These partnerships would focus on creating sustainable cost structures that make quality healthcare accessible to rural populations while maintaining fiscal responsibility. The network should utilize Health Level Seven's (HL7) interoperability standards to enable seamless data sharing between rural health hubs, telehealth platforms, and traditional healthcare facilities, ensuring vendor-neutral connectivity across the innovation network. The initiative would include the development of AI-enabled mobile integrated care that can bring advanced medical capabilities directly to rural communities, reducing the need for long-distance travel to receive care. The program would also establish partnerships with local businesses and community organizations to create health promotion programs that address social determinants of health in rural areas.

This initiative also would advance a voluntary federal licensure framework specifically for FQHC providers, enabling them to practice across state lines while serving federal health program beneficiaries. The agencies should implement standardized, AI-powered credentialing verification systems that enable rapid provider onboarding across the FQHC network while maintaining appropriate safety standards. This reform would enable FQHCs and AI-powered care teams to rapidly expand their reach, particularly in rural areas, ensuring that no patient is left behind due to geographic limitations. AI-powered credentialing verification systems would further streamline provider onboarding across this expanded network, ensuring rapid deployment of specialists and care teams to areas of need. By combining technology-driven care delivery with streamlined provider mobility, this initiative would reduce administrative burden, lower costs, and improve healthcare access at scale.

ACTION IN SUM

Through an AI-enabled care network connecting thousands of FQHCs, health systems, and academic medical centers nationwide, patients with complex conditions like heart failure could access top-tier specialist care regardless of location, with AI-powered screening and remote monitoring enabling early intervention by leading specialists across state lines, while mobile diagnostic units provide rapid in-person care when needed, potentially preventing hundreds of thousands of hospitalizations annually and dramatically improving outcomes for traditionally underserved populations.

Implement AI-Driven Measurements To Eliminate Waste and Red Tape

CMS can develop and implement an AI-powered system for measuring healthcare quality that fundamentally shifts focus from process metrics to actual patient outcomes, thereby eliminating excessive administrative red tape and waste. As the U.S. continues to shift away from fee-for-service, properly attributing costs and outcomes across complex patient journeys is becoming increasingly difficult and convoluted, which are issues AI can help resolve.

This system would use machine learning algorithms to analyze multiple data sources in near-real-time, including electronic health records, claims data, patient-reported outcomes, and social determinants of health in near-real time, reducing administrative burden as well as wasteful effort and spending in healthcare. Natural language processing (NLP) would extract meaningful insights from unstructured clinical notes and patient feedback, providing a more complete picture of care quality. The platform would also include predictive analytics capabilities to identify potential quality issues before they impact patient care, enabling proactive interventions.

Healthcare providers would actively participate in defining meaningful quality metrics that reflect real-world clinical practice and patient needs, moving beyond traditional Healthcare Effectiveness Data and Information Set (HEDIS) measures, a set of standardized measures used by more than 90 percent of extant U.S. health plans. These collaborations would ensure that quality measurements are both clinically relevant and actionable, while technology companies would develop the necessary AI tools to capture and analyze this data efficiently. The system would include automated feedback loops that continuously refine quality metrics based on observed outcomes and changing healthcare practices. Regular validation studies would ensure that AI-generated quality assessments align with clinical expertise and super patient-first experiences.

The system would provide automated feedback loops, continuously refining quality metrics based on real-world outcomes and healthcare trends. This would include developing standardized approaches for translating quality data into actionable recommendations for healthcare providers and administrators. The system would also incorporate mechanisms for sharing best practices across healthcare organizations, as well as identifying wasteful efforts and wasteful spending both locally and nationally, thereby creating a learning network that accelerates quality improvement efforts. Regular assessments would measure both the accuracy of AI-generated quality metrics and their impact on patient outcomes and healthcare costs.

ACTION IN SUM

Millions of beneficiaries with complex conditions like chronic kidney disease and heart disease, healthcare organizations could precisely track treatment effectiveness, optimize resource allocation, and align payments with actual health outcomes rather than process metrics, saving billions in care costs while dramatically improving quality of life for patients through better coordinated care across specialties and more accurate value-based reimbursement models that incentivize proven interventions.

This action would establish next-generation AI-powered systems for measuring healthcare quality that shifts focus from process measures to actual patient outcomes through near real-time analysis. This initiative primarily supports Pillar 2, needed innovations without red tape, in addition to Pillars 1 and 4, catalyzing better health outcomes while expediting fiscal responsibility through improved quality measurement.

Launch an Interoperable, State-Based Health Data Infrastructure

HHS, in partnership with the 50 different states, can advance the development of a revolutionary, secure, and interoperable state-based health data infrastructure that leverages advanced AI capabilities for near real-time analysis and sharing of health information across the healthcare ecosystem. This comprehensive system would incorporate state-of-the-art encryption technologies to ensure patient privacy while enabling seamless coordination between healthcare providers, researchers, and public health officials. The infrastructure would include AI-powered predictive analytics capabilities that can identify population health trends and potential public health emergencies before they become critical. The system would also feature automated compliance monitoring to ensure adherence to all relevant privacy regulations and security standards. Additionally, the platform would incorporate machine learning algorithms that continuously improve data quality and accuracy through automated validation and correction processes.

Private sector technology companies would collaborate extensively with HHS to develop the secure, scalable platforms necessary for this state-based infrastructure, bringing expertise in cloud computing, distributed systems, and advanced security protocols. These partnerships would facilitate the creation of standardized APIs and data exchange protocols that enable seamless integration across different healthcare systems and platforms. The infrastructure should leverage HL7's established interoperability standards and frameworks to ensure consistent, vendor-neutral data exchange across state-based healthcare ecosystems while enabling AI-powered analytics capabilities. The private sector would also contribute innovative solutions for data anonymization and aggregation, ensuring that valuable health insights can be derived while maintaining individual privacy. The same data-driven approaches also will help identify fraud and wasteful spending in healthcare. Healthcare providers would participate in extensive testing and validation processes to ensure the system meets their operational needs while maintaining efficiency in patient care delivery.

This transformative initiative would establish clear protocols for data governance, access controls, and audit trails, ensuring transparency and accountability in how health data is used and shared. The system would include robust disaster recovery and business continuity features to ensure uninterrupted access to critical health information during emergencies. Regular security assessments and penetration testing would be conducted to identify and address potential vulnerabilities. The initiative would also include comprehensive training programs to help healthcare providers and administrators effectively utilize the new infrastructure.

ACTION IN SUM

A world-leading, secure, and interoperable health data infrastructure connecting all fifty states improves health for both acute and chronic diseases, for example U.S. children at risk for diabetes, enabling unprecedented improvements in disease prevention and personalized care delivery while maintaining robust privacy protections.

This action would advance a revolutionary, secure, and interoperable state-based health data infrastructure for the U.S. that would be best in-class for the world, enabling analysis and sharing of health information while maintaining patient privacy. This initiative primarily supports Pillars 2 and 3, advancing innovation and revolutionizing patient-first care, while also contributing to Pillar 4 through improved system efficiency.

Advance Comprehensive Cost-Saving Preventive Care Programs

CMS can implement a revolutionary, data-driven cost-saving preventive care initiative that leverages advanced AI analytics to identify at-risk populations and intervene before health conditions become severe. The system would analyze value-based healthcare outcomes and ultimately health outcomes, including social determinants of health, environmental factors, and lifestyle choices, aligned with the focus of the 'Make America Healthy Again' initiative on addressing root causes of chronic disease. This comprehensive approach would incorporate near real-time monitoring of population health trends, enabling healthcare providers to allocate resources more effectively and target interventions where they're needed most. The program would also include AI-powered patient engagement tools that provide personalized health recommendations and reminders, making preventive care more accessible and engaging for all populations.

Healthcare providers would collaborate with technology partners to develop and implement targeted interventions based on AI-generated insights, creating a more proactive healthcare delivery system. These partnerships would facilitate the development of innovative care delivery models that emphasize prevention over treatment, while ensuring that interventions are culturally appropriate and accessible to all populations. The cost-saving, quality measurement approaches should incorporate HL7's standardized data formats and exchange protocols to ensure consistent quality metrics collection and reporting across different healthcare providers and systems. The program would include continuous monitoring and evaluation of intervention effectiveness, with AI systems automatically adjusting recommendations based on observed outcomes and new data. Regular feedback loops between providers and AI systems would ensure that interventions remain relevant and effective.

The initiative would establish clear metrics for measuring the success of preventive interventions, including both short-term health improvements and long-term cost savings. This would involve creating sophisticated AI models that can predict the long-term impact of preventive measures on population health and healthcare costs. The program would also include mechanisms for sharing successful intervention strategies across healthcare systems, creating a learning network that continuously improves preventive care delivery. This action primarily supports Pillars 1 and 4 by catalyzing better health outcomes while reducing long-term healthcare costs through prevention.

ACTION IN SUM

Through AI-powered early detection and intervention systems deployed across thousands of workplaces nationwide, millions of workers at risk for musculoskeletal conditions could receive personalized prevention plans and timely care interventions, potentially preventing hundreds of thousands of costly surgeries annually while improving workforce mobility and productivity through data-driven, value-based care delivery that combines virtual and in-person therapeutic options to dramatically reduce both human suffering and healthcare costs.

This action would implement comprehensive preventive care initiatives using AI analytics to identify populations at risk and enable early interventions. This initiative primarily supports Pillars 1 and 4 by catalyzing better health outcomes while reducing long term healthcare costs through prevention, in addition to supporting Pillar 3, prioritizing patient-first care.

Accelerate Training for AI-Empowered Healthcare Workers

HHS can create a groundbreaking program to prepare the next generation of healthcare workers for an AI-augmented healthcare environment, fundamentally transforming how medical professionals are trained and their role. This comprehensive initiative would include partnerships with medical schools, technology companies, and healthcare providers to develop innovative curriculum and practical training programs that blend traditional medical knowledge with advanced AI capabilities. The program would create new categories of AI-enabled healthcare professionals while ensuring that core medical skills remain strong and central to healthcare delivery. The initiative would also include specialized tracks for different healthcare roles, from physicians to nurses to clinical support staff.

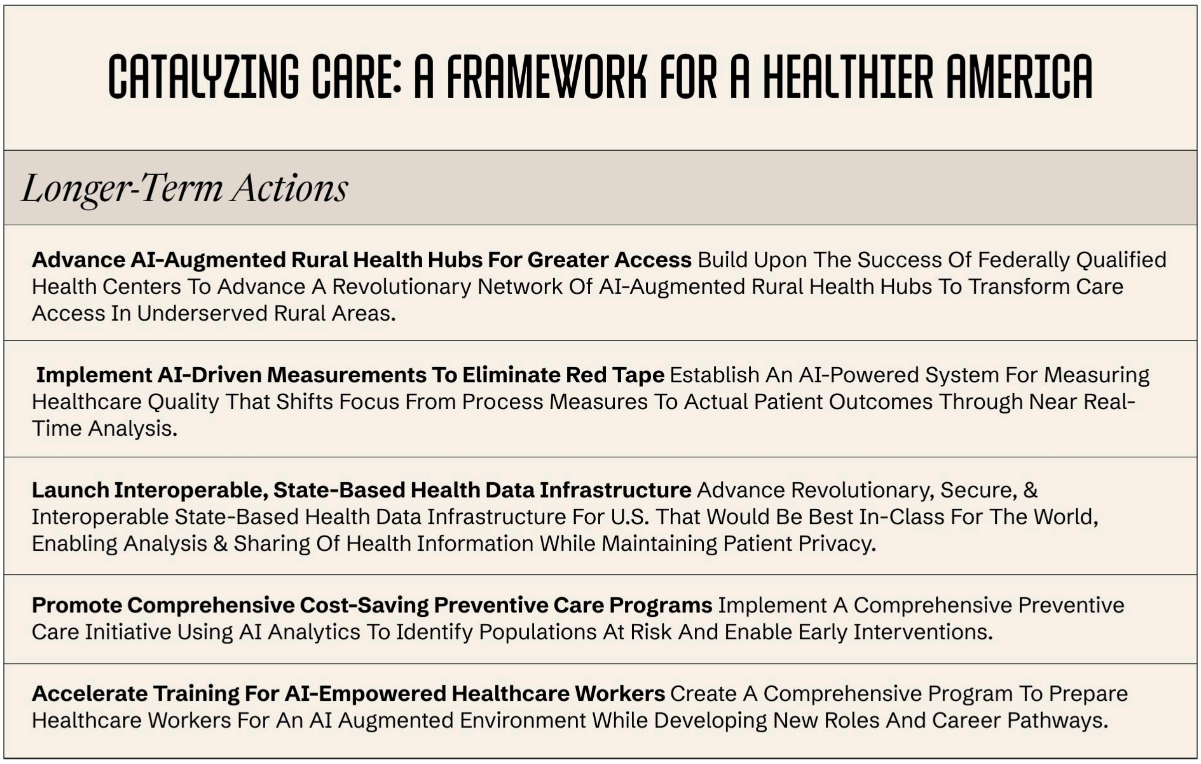
The private sector would play a crucial role in providing real-world use cases, technology platforms, and expertise in AI implementation. These partnerships would ensure that training programs remain current with the latest technological advances and industry needs. Technology companies would contribute by developing specialized training modules and simulation environments that allow healthcare workers to gain hands-on experience with AI tools in a safe, controlled setting. Healthcare providers would provide feedback on practical implementation challenges and success stories, helping to refine and improve the training programs.

Educational institutions would integrate AI training into their existing programs while developing new specialized courses and certifications for AI-enabled healthcare roles. This would include creating standardized competency frameworks for distinct levels of AI proficiency in healthcare settings. The program would establish clear career pathways for healthcare professionals looking to specialize in AI-enabled care delivery, including opportunities for continuing education and professional development. Regular assessments would measure both technical proficiency and practical application skills, ensuring healthcare workers can effectively integrate AI tools into their daily workflows.

ACTION IN SUM

AI training programs would equip healthcare workers to use AI-powered diagnostics and streamline workflows, freeing up time to spend with patients and increasing access to care. Health providers will have defined career paths to develop AI expertise through training and advancement opportunities, benefitting their patients with superior healthcare delivery.

This action would create a comprehensive program to prepare healthcare workers for an AI augmented environment while developing new roles and career pathways. This initiative primarily supports Pillar 5, strengthening U.S. medical talent, while also contributing to Pillars 1 and 2 through improved healthcare delivery capabilities.



CATALYZING CARE: A FRAMEWORK FOR A HEALTHIER AMERICA

Longer-Term Actions
Advance AI-Augmented Rural Health Hubs For Greater Access Build Upon The Success Of Federally Qualified Health Centers To Advance A Revolutionary Network Of AI-Augmented Rural Health Hubs To Transform Care Access In Underserved Rural Areas.
Implement AI-Driven Measurements To Eliminate Red Tape Establish An AI-Powered System For Measuring Healthcare Quality That Shifts Focus From Process Measures To Actual Patient Outcomes Through Near Real-Time Analysis.
Launch Interoperable, State-Based Health Data Infrastructure Advance Revolutionary, Secure, & Interoperable State-Based Health Data Infrastructure For U.S. That Would Be Best In-Class For The World, Enabling Analysis & Sharing Of Health Information While Maintaining Patient Privacy.
Promote Comprehensive Cost-Saving Preventive Care Programs Implement A Comprehensive Preventive Care Initiative Using AI Analytics To Identify Populations At Risk And Enable Early Interventions.
Accelerate Training For AI-Empowered Healthcare Workers Create A Comprehensive Program To Prepare Healthcare Workers For An AI Augmented Environment While Developing New Roles And Career Pathways.

Figure 4. Longer-Term Actions

A CLEAR PATH FORWARD

The moment for transformative action to advance U.S. healthcare that works is now. Through dynamic market-driven approaches, we can and will harness innovative technology while championing value-based healthcare outcomes and ensuring patient safety through 'radical transparency' in healthcare delivery systems. By embracing patient-first care, data, and accessibility, implementing prudent fiscal practices, and mobilizing U.S. talent, we can achieve transformation through market-driven innovation. This bold transformation will be achieved through the five pillars for Catalyzing Care: A Framework for a Healthier America that rally market-driven approaches – collectively with startups, educational institutions and other partners working alongside federal and state governments – to deliver U.S. healthcare that works for all Americans.

GLOSSARY OF TERMS

AI - Artificial Intelligence
ASTP - Assistant Secretary for Technology Policy
CMS - Centers for Medicare & Medicaid Services
EHR - Electronic Health Records
FDA - Food and Drug Administration
FHIR - Fast Healthcare Interoperability Resources
FQHC - Federally Qualified Health Centers
HHS - Department of Health and Human Services
HL7 - Health Level Seven
HTI-1 - Health Data, Technology, and Interoperability
ICU - Intensive Care Unit
NLP - Natural Language Processing
ONC - Office of the National Coordinator

ABOUT GCI

General Catalyst is a global investment and transformation company that partners with the world's most ambitious entrepreneurs to drive resilience and applied AI. Launched in 2024, the General Catalyst Institute's (GCI) mission is to promote and strengthen national resilience around the world by backing transformative technologies and shaping public policies that improve society. GCI's top priority is cultivating a healthy ecosystem for entrepreneurship and serving as a trusted partner to the global policymaking community on how to respond, leverage and adopt cutting-edge technology, such as applied AI. The institute operates as a hub for collaboration and partnership between entrepreneurs, government, investors, experts and academics to help shape informed policy solutions. Visit us at www.generalcatalyst.com/GCI.

ACKNOWLEDGEMENTS

The General Catalyst Institute (GCI) wishes to express its appreciation to the many health technology innovators and policy experts who shared expertise and insights for the paper prior to its publication. In particular, GCI expresses gratitude to the leadership of General Catalyst including Hemant Taneja, Chris Bischoff, Daryl Tol for their vision and guidance, as well as Candace Richardson and Jack Cohen for their efforts. Special thanks are extended as well to the many General Catalyst portfolio companies and partners with whom we consulted throughout this process - we are grateful for the work they do everyday to dedicate themselves to improving health outcomes by driving transformation in communities across the United States.

Artificial Intelligence and Synthetic Biology Are Not Harbingers of Doom

> **To advance research in biotechnology and AI, the private and public sectors must take actions to remedy perceptions of benevolence, competence, and integrity**

By David Bray
Grand Strategy

November 20, 2023

Contrary to many people's fears, artificial intelligence (AI) can be a positive force in advancing biological research and biotechnology. The assumption that AI will super-empower the risks that already exist for the misuse of biotech to develop and spread pathogens and fuel bioterrorism misses three key points. First, the data must be out there for either an AI or a human to use it. Second, governments stop bad actors from using bio for nefarious purposes by focusing on the actors' precursor behaviors. Third, given how wrong large language models (LLMs) often are and their risk of hallucinations, any would-be AI intended to provide advice on biotech will have to be checked by a human expert. In contrast, AI can be a positive force in advancing biological research and biotechnology — and insights from biology can power the next wave of AI for the benefit of humankind. Private and public-sector leaders need to make near-term decisions and actions to lay the foundation for maximizing the

benefits of AI and biotech. National and international attention should focus on both new, collective approaches to data curation and ensuring the right training approaches for AI models of biological systems.

THE RED CELL PROJECT

The Red Cell series is published in collaboration with The National Interest. Drawing upon the legacy of the CIA's Red Cell—established following the September 11 attacks to avoid similar analytic failures in the future—the project works to challenge assumptions, misperceptions, and groupthink with a view to encouraging alternative approaches to America's foreign and national security policy challenges.

Are AI and biological research harbingers of certain doom — or awesome opportunities?

Contrary to the reigning assumption that artificial intelligence (AI) will super-empower the risks of misuse of biotech to create pathogens and bioterrorism, AI holds the promise of advancing biological research, and biotechnology can power the next wave of AI to greatly benefit humanity. Worries about the misuse of biotech are especially prevalent, recently prompting the Biden administration to publish guidelines for biotech research, in part to calm growing fears.

The doomsday assumption that AI will inevitably create new, malign pathogens and fuel bioterrorism misses three key points. First, the data must be out there for an AI to use it. AI systems are only as good as the data they are trained upon. For an AI to be trained on biological data, that data must first exist — which means it is available for humans to use with or without AI. Moreover, attempts at solutions that limit access to data overlook the fact that biological data can be discovered by researchers and shared via encrypted form absent the eyes or controls of a government. No solution attempting to address the use of biological research to develop harmful pathogens or bioweapons can rest on attempts to control either access to data or AI because the data will be discovered and will be known by human experts regardless of whether any AI is being trained on the data.

Second, governments stop bad actors from using biotech for bad purposes by focusing on the actors' precursor behaviors to develop a bioweapon; fortunately, those same techniques work perfectly well here, too. To mitigate the risks that bad actors — be they human or humans and machines combined — will misuse AI and biotech, indicators and warnings need to be developed. When advances in technology, specifically steam engines, concurrently resulted in a new type of crime, namely train robberies, the solution was not to forego either steam engines or their use in conveying cash and precious cargo. Rather, the solution was to employ other improvements, to later include certain types of safes that were harder to crack and subsequently, dye packs to cover the hands and clothes of robbers. Similar innovations in early warning and detection are needed today in the realm of AI and biotech, including developing methods to warn about reagents and activities, as well as creative means to warn when biological research for negative ends is occurring.

This second point is particularly key given the recent Executive Order (EO) released on 30 October 2023 prompting U.S. agencies and departments that fund life-science projects to establish strong, new standards for biological synthesis screening "as a condition of federal funding . . . [to] manage risks potentially made worse by AI." Often the safeguards to ensure any potential dual-use biological research is not misused involve monitoring the real world to provide indicators and early warnings of potential ill-intended uses. Such an effort should involve monitoring for early indicators of potential ill-intended uses the way governments employ monitoring to stop bad actors from misusing any dual-purpose scientific endeavor. Although the recent EO is not meant to constrain research, any attempted solutions limiting access to data miss the fact that biological data can already be discovered and shared via encrypted forms beyond government control. The same techniques used today to detect malevolent intentions will work whether large language models (LLMs) and other forms of Generative AI have been used or not.

Third, given how wrong LLMs and other Generative AI systems often are, as well as the risks of generating AI hallucinations, any would-be AI intended to provide advice on biotech will have to be checked by a human expert. Just because an AI can generate possible suggestions and formulations — perhaps even suggest novel formulations of new pathogens or biological materials — it does not mean that what the AI has suggested has any grounding in actual science or will do biochemically what the AI suggests the designed material could do. Again, AI by itself does not replace the need for human knowledge to verify whatever advice, guidance, or instructions are given regarding biological development is accurate.

Moreover, AI does not supplant the role of various real-world patterns and indicators to tip off law enforcement regarding potential bad actors engaging in biological techniques for nefarious purposes. Even before advances in AI, the need to globally monitor for signs of potential biothreats, be they human-produced or natural, existed. Today with AI, the need to do this in ways that still preserve privacy while protecting societies is further underscored.

Knowledge of how to do something is not synonymous with the expertise in and experience in doing that thing: Experimentation and additional review. AIs by themselves can convey information that might foster new knowledge, but they cannot convey expertise without months of a human actor doing silica (computer) or in situ (original place) experiments or simulations. Moreover, for governments wanting to stop malicious AI with potential bioweapon-generating information, the solution can include introducing uncertainty in the reliability of an AI system's outputs. Data poisoning of AIs by either accidental or intentional means represents a real risk for any type of system. This is where AI and biotech can reap the biggest benefit. Specifically, AI and biotech can identify indicators and warnings to detect risky pathogens, as well as to spot vulnerabilities in global food production and climate-change-related disruptions to make global interconnected systems more resilient and sustainable. Such an approach would not require massive intergovernmental collaboration before researchers could get started; privacy-preserving approaches using economic data, aggregate (and anonymized) supply-chain data, and even general observations from space would be sufficient to begin today.

Why communities should care about how AI can advance biological research — and how biology can power the next wave of AI

Setting aside potential concerns regarding AI being used for ill-intended purposes, the intersection of biology and data science is an underappreciated aspect of the last two decades. At least two COVID-19 vaccinations were designed in a computer — and were then printed nucleotides via an mRNA printer. Had this technology not been possible, it might have taken an additional two or three years for the same vaccines to be developed. Even more amazing, nuclide printers presently cost only $500,000 and will presumably become less expensive and more robust in their capabilities in the years ahead.

AI can benefit biological research and biotechnology, provided that the right training is used for AI models. To avoid downside risks, it is imperative that new, collective approaches to data curation and training for AI models of biological systems be made in the next few years.

As noted earlier, much attention has been placed on both AI and advancements in biological research; some of these advancements are based on scientific rigor and backing; others are driven more by emotional excitement or fear. When setting a solid foundation for a future based on values and principles that support and safeguard all people and the planet, neither science nor emotions alone can be the guide. Instead, considering how projects involving biology and AI can build and maintain trust — despite the challenges of both intentional disinformation and accidental misinformation — can illuminate a positive path forward.

> The concerns regarding the potential for AI and biology to be used for ill-intended purposes should not overshadow the present conversations about using technologies to address important regional and global issues.

Specifically, in the last few years, attention has been placed on the risk of an AI system training novice individuals how to create biological pathogens. Yet this attention misses the fact that such a system is only as good as the data sets provided to train it; the risk already existed with such data being present on the internet or via some other medium. Moreover, an individual cannot gain from an AI the necessary experience and expertise to do whatever the information provided suggests — such experience only comes from repeat coursework in a real-world setting. Repeat work would require access to chemical and biological reagents, which could alert law enforcement authorities. Such work would also yield other signatures of preparatory activities in the real world.

Others have raised the risk of an AI system learning from biological data and helping to design more lethal pathogens or threats to human life. The sheer complexity of different layers of biological interaction, combined with the risk of certain types of generative AI to produce hallucinated or inaccurate answers — as this article details in its concluding section — makes this not as big of a risk as it might initially seem. Specifically, the risks from expert human actors working together across disciplines in a concerted fashion represent a much more significant risk than a risk from AI, and human actors working for ill-intended purposes together (potentially with machines) presumably will present signatures of their attempted activities. Nevertheless, these concerns and the mix of both hype and fear surrounding them underscore why communities should care about how AI can benefit biological research.

HOW CAN A SOLID FOUNDATION FOR BOTH AI AND BIOLOGY FOR THE NEXT TWO DECADES BE ESTABLISHED?

The merger of data and bioscience is one of the most dynamic and consequential elements of the current tech revolution. A human organization, with the right goals and incentives, can accomplish amazing outcomes ethically, as can an AI. Similarly, with either the wrong goals or wrong incentives, an organization or AI can appear to act and behave unethically. To address the looming impacts of climate change and the challenges of food security, sustainability, and availability, both AI and biological research will need to be employed. For example, significant amounts of nitrogen have already been lost from the soil in several parts of the world, resulting in reduced agricultural yields. In parallel, methane gas is a pollutant that is between 22 and 40 times worse — depending on the scale of time considered — than carbon dioxide in terms of its contribution to the Greenhouse Effect impacting the planet. Bacteria generated through computational means can be developed through natural processes that use methane as a source of energy, thus consuming and removing it from contributing to the Greenhouse Effect, while simultaneously returning nitrogen from the air to the soil, thereby making the soil more productive in producing large agricultural yields.

The concerns regarding the potential for AI and biology to be used for ill-intended purposes should not overshadow the present conversations about using technologies to address important regional and global issues. To foster global activities to help both encourage the productive use of these technologies for meaningful human efforts — and ensure ethical applications of the technologies in parallel — an existing group, namely the international Genetically Engineered Machine (iGEM) competition, should be expanded. Specifically, iGEM represents a global academic competition, which started in 2004, aimed at improving understanding of synthetic biology while also developing an open community and collaboration among groups. In recent years, over 6,000 students in 353 teams from 48 countries have participated. Expanding iGEM to include a track associated with categorizing and monitoring the use of synthetic biology “for good” as well as working with national governments on ensuring that such technologies are not used for ill-intended purposes would represent two great ways to move forward.

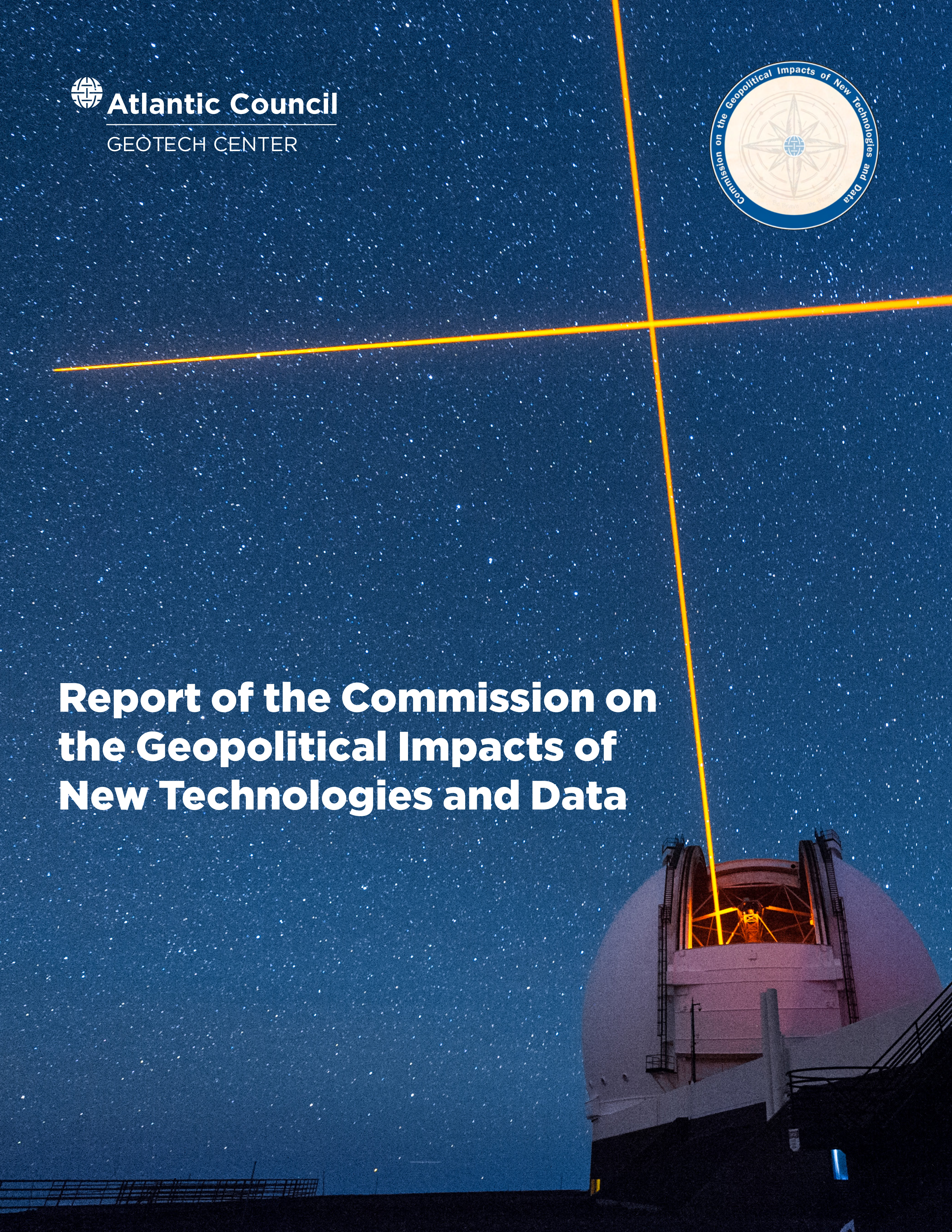
As for AI in general, when considering governance of AIs, especially for future biological research and biotechnology efforts, decisionmakers would do well to consider both existing and needed incentives and disincentives for human organizations in parallel. It might be that the original Turing Test — designed by computer science pioneer Alan Turing — intended to test whether a computer system is behaving intelligently, is not the best test to consider when gauging local, community, and global trust. Specifically, the original test involved Computer A and Person B, with B attempting to convince an interrogator, Person C, that they were human, and that A was not. Meanwhile, Computer A was trying to convince Person C that they were human.

Consider the current state of some AI systems, where the benevolence of the machine is indeterminate, competence is questionable because some AI systems are not fact-checking and can provide misinformation with apparent confidence and eloquence, and integrity is absent. Some AI systems can change their stance if a user prompts them to do so.

However, these crucial questions regarding the antecedents of trust should not fall upon these digital innovations alone — these systems are designed and trained by humans. Moreover, AI models will improve in the future if developers focus on enhancing their ability to demonstrate benevolence, competence, and integrity to all. Most importantly, consider the other “obscured boxes” present in human societies, such as decision-making in organizations, community associations, governments, oversight boards, and professional settings – such as decision-making in organizations, community associations, governments, oversight boards, and professional settings. These human activities also will benefit by enhancing their ability to demonstrate benevolence, competence, and integrity to all in ways akin to what we need to do for AI systems as well.

Ultimately, to advance biological research and biotechnology and AI, private and public-sector efforts need to take actions that remedy the perceptions of benevolence, competence, and integrity (i.e., trust) simultaneously.

David Bray *is Co-Chair of the Loomis Innovation Council and a Distinguished Fellow at the Stimson Center.*



Atlantic Council

GEOTECH CENTER

Report of the Commission on the Geopolitical Impacts of New Technologies and Data

Atlantic Council

GEOTECH CENTER

The Atlantic Council GeoTech Center works to shape the global future of data and technology together.

ISBN-13: 978-1-61977-178-9

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report’s conclusions.

May 2021

Cover: Double Keck Lasers by Jason Chu Photography, https://jason-chu.pixels.com

Website: This report includes an interactive website, https://atlanticcouncil.org/geotechreport

Commission on the Geopolitical Impacts of New Technologies and Data

In preparing this report for the United States and its allies, to include members of Congress, the new presidential administration, private industry, academia, and like-minded nations, the Commission on the Geopolitical Impacts of New Technologies and Data sought to provide a compass bearing between where the world stood in 2020-2021 and a freer, more secure, and more prosperous world in 2031.

Data capabilities and new technologies impact geopolitics, global competition, and global opportunities for collaboration. The coming decade must address the sophisticated but potentially fragile systems that now connect people and nations, and incorporate resiliency as a necessary foundational pillar of modern life. To maintain national and economic security and competitiveness in the global economy, the United States and its allies must continue to be preeminent in key technology areas, and take measures to ensure the trustworthiness and sustainability of the digital economy, the analog economy, and their infrastructures to include:

- **Global science and technology leadership**
- **Secure data and communications**
- **Enhanced trust and confidence in the digital economy**
- **Assured supply chains and system resiliency**
- **Continuous global health protection and global wellness**
- **Assured space operations for public benefit**
- **Future of work**

The report's practical, implementable recommendations will enable the United States and like-minded nations to employ data capabilities and new technologies to achieve the goals set by this Commission.

John B. Goodman
Mr. John Goodman, Co-Chair

Teresa A. Carlson
Ms. Teresa Carlson, Co-Chair

David A. Bray, Director

Co-Chairs
Mr. John Goodman
Ms. Teresa Carlson

Honorary Co-Chairs
Sen. Mark Warner
Sen. Rob Portman
Rep. Suzan DelBene
Rep. Michael McCaul

Commissioners
Mr. Max R. Peterson II
Mr. Paul Daugherty
Mr. Maurice Sonnenberg
Hon. Michael Chertoff
Hon. Michael J. Rogers
Mr. Pascal Marmier
Ramayya Krishnan, PhD
Hon. Shirley Ann Jackson, PhD
Hon. Susan M. Gordon
Vint Cerf, PhD
Zia Khan, PhD
Anthony Scriffignano, PhD
Ms. Frances F. Townsend
Admiral James Stavridis, USN, Ret.

Director & Executive Team
David A. Bray, PhD
Peter Brooks, PhD
Ms. Stephanie Wander

Executive Summary

The advancing speed, scale, and sophistication of new technologies and data capabilities that aid or disrupt our interconnected world are unprecedented. While generations have relied consistently on technologies and tools to improve societies, we now are in an era where new technologies and data reshape societies and geopolitics in novel and even unanticipated ways. As a result, governments, industries, and other stakeholders must work together to remain economically competitive, sustain social welfare and public safety, protect human rights and democratic processes, and preserve global peace and stability.

Emerging technologies also promise new abilities to make our increasingly fragile global society more resilient. To sustain this progress, nations must invest in research, expand their digital infrastructures, and increase digital literacy so that their people can compete and flourish in this new era. Yet, at the same time, no nation or international organization is able to keep pace with the appropriate governance structures needed to grapple with the complex and destabilizing dynamics of these emerging technologies. Governments, especially democratic governments, must work to build and sustain the trust in the algorithms, infrastructures, and systems that could underpin society. The world must now start to understand how technology and data interact with society and how to implement solutions that address these challenges and grasp these opportunities. Maintaining both economic and national security and resiliency requires new ways to develop and deploy critical and emerging technologies, cultivate the needed human capital, build trust in the digital fabric with which our world will be woven, and establish norms for international cooperation.

The Commission on the Geopolitical Impacts of New Technologies and Data (GeoTech Commission) was established by the Atlantic Council in response to these challenges and seeks to develop recommendations to achieve these strategic goals. Specifically, the GeoTech Commission examined how the United States, along with other nations and global stakeholders, can maintain science and technology (S&T) leadership, ensure the trustworthiness and resiliency of physical and software/informational technology (IT) supply chains and infrastructures, and improve global health protection and wellness. The GeoTech Commission identified key recommendations and practical steps forward for the US Congress, the presidential administration, executive branch agencies, private industry, academia, and like-minded nations.

The GeoTech Decade

Data capabilities and new technologies increasingly exacerbate social inequality and impact geopolitics, global competition, and global opportunities for collaboration. The coming decade—the "GeoTech Decade"—must address the sophisticated but potentially fragile systems that now connect people and nations, and incorporate resiliency as a necessary foundational pillar of modern life. Additionally, the rapidity of machines to make sense of large datasets and the speed of worldwide communications networks means that any event can escalate and cascade quickly across regions and borders—with the potential to further entrench economic inequities, widen disparities in access to adequate healthcare, as well as to hasten increased exploitation of the natural environment. The coming years also will present new avenues for criminals and terrorists to do harm; authoritarian nations to monitor, control, and oppress their people; and diplomatic disputes to escalate to armed conflict not just on land, sea, and in the air, but also in space and cyberspace.

2001-2011

Decade of Counterterrorism activities globally

2011-2021

Decade of Decreasing Trust in government and big technology companies

2021-2031

GeoTech Decade where technology and new data capabilities will significantly affect geopolitics, competition, and collaboration

Domestically and internationally, the United States must promote strategic initiatives that employ data and new technologies to amplify the ingenuity of people, diversity of talent, strength of democratic values, innovation of companies, and the reach of global partnerships.

Geopolitical Impacts of New Technologies and Data Collections

Critical technologies that will shape the GeoTech Decade—and in which the United States and its allies must maintain global S&T leadership—can be grouped into six areas. All technologies in these categories will have broad—and interdependent—effects on people and the way they live and work, on global safety and security, and on the health of people and our planet.

- **Technologies that enable a digital economy: communications and networking, data science, and cloud computing:** collectively provide the foundation for secure transmission of data for both the public and private sector and establish robust economies of ideas, resources, and talent.
- **Technologies for intelligent systems: artificial intelligence, distributed sensors, edge computing, and the Internet of Things:** add new capabilities for

understanding changes in the world in both physical and digital environments. The resulting data may supplement human intelligence, social engagements, and other sources of insight and analysis. In select, defined areas, intelligent systems may enhance human governance of complex systems or decisions.

- **Technologies for global health and wellness: biotechnologies, precision medicine, and genomic technologies:** help create new fields of research, development, and practical solutions that promote healthy individuals and communities. Nations and health care organizations can use advances in genomics, or more broadly omics,[1] to provide sentinel surveillance[2] capabilities with respect to natural or weaponized pathogens. Sentinel surveillance can provide early detection, data about how a new element is appearing and growing, and information to guide our response.

- **Technologies that enlarge where people, enterprises, and governments operate: space technologies, undersea technologies:** commercial companies and nations around the world are deploying mega-constellations of satellites, or fleets of autonomous ocean platforms, with advanced, persistent surveillance and communications capabilities. Large-scale Earth observation data is important for monitoring the world's atmosphere, oceans, and climate as a foundation for understanding evolving health and environmental risks and increasing the economic efficiencies in transportation, agriculture, and supply chain robustness.

- **Technologies that augment human work: autonomous systems, robotics, and decentralized energy methods:** collectively provide the foundation to do work in dangerous or hazardous environments without risk to human lives, while at the same time augmenting human teams, potentially prompting long-term dislocations in national workforces, and requiring additional workforce talent for new technology areas.

- **Foundational technologies: quantum information science (QIS), nanotechnology, new materials for extreme environments, and advanced microelectronics:** collectively provide the foundation for solving classes of computational problems, catalyzing next-generation manufacturing, setting standards, creating new ways to monitor the trustworthiness of digital and physical supply chains, as well

[1] Omics technologies are primarily aimed at the universal detection of genes (genomics), mRNA (transcriptomics), proteins (proteomics), and metabolites (metabolomics) in a specific biological sample.

[2] A sentinel surveillance system is used to obtain data about a particular disease that cannot be obtained through a passive system such as summarizing standard public health reports. Data collected in a well-designed sentinel system can be used to signal trends, identify outbreaks, and monitor disease burden, providing a rapid, economical alternative to other surveillance methods. Source: "Immunization Analysis and Insights," World Health Organization, accessed March 19, 2021, https://www.who.int/teams/immunization-vaccines-and-biologicals/immunization-analysis-and-insights/surveillance/surveillance-for-vpds.

as potentially presenting new challenges and opportunities to communications security that underpin effective governance and robust economies.

In addition to the technology itself, countries and organizations must learn to harness and protect the human element—by recruiting and upskilling workers with the needed skill sets for today and training the next generation with the right knowledge for tomorrow. There is great competition globally for digitally-skilled workers, and some countries or companies invest large amounts to develop or recruit this talent. When like-minded nations collaborate in S&T areas, the talent resources can produce greater benefits than possible otherwise. This requires governments to ensure their entire populations gain the needed digital literacy skills and have the means and opportunities to participate in the global digital economy. Making the whole greater than the sum of the parts represents the important global need for international collaboration.

The broad range of important S&T areas requires several forms of collaboration. In multiple key areas, such as QIS and advanced microelectronics, several nations already have significant government investments underway, and current results span a growing number of application areas. Collaborating on research and coordinating national investments among like-minded nations could benefit all participants. Fast-evolving technical capabilities, such as commercial space or autonomous systems, are supporting global industries that are developing and fielding new products. Effective collaboration relies on a broad ecosystem of domestic and foreign partners, including private sector entities. Collaboration will be limited in certain areas, for example, areas where, due to security considerations, the United States will develop capabilities in a self-reliant manner.

Table ES.1: The GeoTech Decade: Areas Where Data and Technology Will Impact Social Equality, Geopolitics, Global Competition, and Global Opportunities for Collaboration

Critical science and technology areas

- Communications and networking, data science, cloud computing
- Artificial intelligence, distributed sensors, edge computing, the Internet of Things
- Biotechnologies, precision medicine, genomic technologies
- Space technologies, undersea technologies
- Autonomous systems, robotics, decentralized energy methods
- Quantum information science, nanotechnology, new materials for extreme environments, advanced microelectronics

Summary of Recommendations

To maintain national and economic security and competitiveness in the global economy, the United States and its allies must

- Continue to be preeminent in key technology areas,
- Take measures to ensure the trustworthiness and sustainability of the digital economy, the analog economy, and their infrastructures.

The GeoTech Commission provides recommendations in the following six areas for achieving these strategic objectives. A seventh area, the Future of Work, discusses ways to ensure the workforce acquires the skills needed for the digital economy, and that there is equitable access to opportunity.

Global science and technology leadership

To ensure that the United States and its allies remain the world leaders in S&T, the federal government, working with industry and stakeholders, should establish a set of prioritized strategic S&T objectives and align those objectives with specific timeframes. Additionally, the United States should establish a technology partnership among like-minded and democratic countries to coordinate actions around those objectives. The president and the US Congress should increase annual federal funding for research and development activities to secure US global leadership in critical new industries and technologies, with priorities determined for the largest impact challenges and gaps. To help people across the United States adapt to the realities of the future, the US government should establish programs to fund reskilling activities for workers displaced by changes brought about by the GeoTech Decade, seek new technologies and increase funding in support of efforts to close the broadband gap, and develop programs to improve the digital literacy of all Americans.

Secure data and communications

To strengthen cybersecurity, the administration should update the implementation plan for the National Cyber Strategy. The strategy should streamline how public and private sector entities monitor the security of their digital environments; encourage new networking, computing, and software designs that strengthen cyber defense; and raise priorities and activities for the cybersecurity of operational technology—the hardware and software that keeps equipment running—to match those of information technology.

Enhanced trust and confidence in the global digital economy

In order maintain the credibility of government and private industry, as well as to ensure prosperity, security, and stability in the coming data-driven epoch, the US government should establish new frameworks for data that incorporate security, accountability, auditability, transparency, and ethics. This means enacting measures that strengthen data privacy and security, establish transparency and ethics principles in how the government and private sector use data about people, and provide guidance on auditing how such data may be used.

Assured supply chains and system resiliency

To ensure that the United States remains attuned to threats and weaknesses in supply chains and critical systems that power its future, the US government should develop a federal mechanism to assess and prioritize the importance of specific supply chains and systems to the nation, considering physical as well as software/IT supply chains and systems. The government should develop procedures and allocate resources to achieve sufficient resiliency, based on these priorities, for supply chains and critical systems to ensure the economic and national security of the United States.

Continuous global health protection and global wellness

In order to protect the American people and environment from future threats, the US government should develop a global early warning system comprised of pandemic surveillance systems coupled with an early warning strategy, as well as a similar system aimed at providing early indicators of global environmental threats which could significantly impact the safety, security, and wellness of the nation.

Assured space operations for public benefit

The US government should foster the growth of the commercial US space industrial base and leverage the increasing capabilities of large commercial satellite constellations. This could increase space mission assurance and deterrence by eliminating mission critical, single-node vulnerabilities and distributing space operations across hosts, orbits, spectrum, and geography.

Table ES.2: Priority Recommendations

1. Global scientific and technology leadership	1.1	Develop a National and Economic Security Technology Strategy
	1.2	Establish a Global GeoTech Alliance and Executive Council
	1.6	Establish national-scale training and education programs to foster continuing technological leadership
2. Secure data and communications	2A.1	Review, update, and reestablish the implementation plan for the National Cyber Strategy
	2A.2	Establish effective and coordinated continuous monitoring for software and hardware used by the federal government
	2A.4	Ensure cybersecurity best practices, expertise, and assurance testing are widely available to industry and government entities
	2B.1	Establish, with other nations, a common set of demonstration milestones for quantum data and communications security
	2B.3	Establish a program to accelerate the operationalization of quantum information science technologies
	2B.4	Establish leading roles for the United States in setting international standards for data and communications security as quantum information science evolves
3. Enhanced trust and confidence in the global digital economy	3.1	Develop a US data privacy standard
	3.4	Empower an organization to audit trust in the digital economy
	3.5	Assess standards relating to the trustworthiness of digital infrastructure
	3.6.	Educate the public on trustworthy digital information
4. Assured supply chains and system resiliency	4.2	Fund and broaden federal oversight of supply chain assurance to include all critical resources
	4.3	For the United States, the administration must develop a geopolitical deterrence strategy that addresses critical digital resources and digital supply chain assurance
	4.4	Conduct regular physical and software/IT supply chain assessments in the United States and with allies, focused on intersecting vulnerabilities with cascading consequences
5. Continuous global health protection and global wellness	5.1	Develop a global early warning system comprised of pandemic surveillance systems coupled with an early warning strategy
	5.4	Increase resilience in medical supply chains
	5.5	Develop capacity building for vaccine and therapeutics discovery, development, and distribution
6. Assured space operations for public benefit	6.2	Foster commercial space technologies of strategic importance and protect these from foreign acquisition
	6.3	Harden the security of commercial space industry facilities and space assets
7. Future of work		Create the workforce for the GeoTech Decade, and equitable access to opportunity

Note: This table contains a subset of the full collection of recommendations.
Numbers refer to the recommendation sequence as discussed in the main chapters of the report.

Table of Contents

Overview: Inflection Points

Accelerating global connectedness—of people, supply chains, networks, economies, the environment, and other foundations of society—is changing how nations work together and compete. For example, the global spread of scientific and technology (S&T) knowledge has lessened the United States' strategic advantage based on advanced technology. The global movement of people allows biological threats to spread worldwide, outpacing the world's ability to respond. In the digital economy, the economic, governmental, and political parts of society are interconnected, with the potential for cybersecurity threats experienced in one context to reverberate in others.

This interconnectedness can lead to inflection points wherein current assumptions and practices are no longer valid or effective. Sources of strength or advantage can diminish. New vulnerabilities can be discovered, e.g., in global supply chains for hardware and software, and exploited. New approaches to protecting national interests in this globally connected world will rely, in many situations, on the cooperation and collaboration of like-minded nations to increase mutual knowledge and awareness. Without this focus, the detrimental aspects of globally connected systems and infrastructures will grow larger and become more urgent.

Each of the following areas is experiencing rapid change and each is critical for ensuring a secure and peaceful world. This overview discusses, for each chapter, the key issues, the opportunities and risks, and a characterization of what must be solved.

Chapter 1: Global Science and Technology Leadership

The United States, with like-minded nations and partners, must collectively maintain continued leadership in key S&T areas to ensure national and economic security, and that technology is developed and deployed with democratic values and standards in mind. The United States must pursue, as strategic goals, establishing priorities, investments, standards, and rules for technology dissemination, developed across government, private industry, academia, and in collaboration with allies and partners. Collaboration among like-minded nations and partners is essential to the attainment of global S&T leadership.

Chapter 2: Secure Data and Communications

Sophisticated attacks on the software/information technology (IT) supply chains have led to significant breaches in the security of government and private networks, requiring a new strategy for cybersecurity. This centers on updating and renewing the National Cyber Strategy Implementation Plan with a focus on streamlining how public and private sector entities monitor their digital environments and exchange information about current threats. Beyond these current challenges, advances in quantum information science (QIS) lay the foundation for future approaches to securing data and communications, to include new ways to monitor the trustworthiness of digital and physical supply chains. With allies and partners, the United States should develop priority global initiatives that employ transformative QIS.

Chapter 3: Enhanced Trust and Confidence in the Global Digital Economy

Diminished trust and confidence in the global digital economy can constrain growth;[3] have destabilizing effects on society, governments, and markets; and lessen resilience against cascading effects of local, regional, or national economic, security, or health instabilities. Trust and confidence are diminished by practices that do not protect privacy or secure data, and by a lack of legal and organizational governance to advance and enforce accountability.[4] Automation and artificial intelligence (AI), essential for digital economies, pose challenges to how we organize and amplify the strength of both while minimizing their weakness or vulnerabilities in open societies. The United States should develop international standards and best practices for a trusted digital economy and should promote adherence to these standards.

Chapter 4: Assured Supply Chains and System Resiliency

Both physical and digital supply chain vulnerabilities can have amplifying effects on the global economy and national security. To protect against these diverse risks requires understanding which types of goods and sectors of the economy are critical, and how to construct supply chains that are inherently more adaptable, resilient, and automated. This requires assessing the state and characteristics of supplies, trade networks and

[3] Congressional Research Service, *Digital Trade and U.S. Trade Policy*, May 21, 2019, 11, accessed March 19, 2021, https://crsreports.congress.gov/product/pdf/R/R44565; in 2015, the Department of Commerce launched a Digital Economy Agenda, Alan B. Davidson, "The Commerce Department's Digital Economy Agenda," November 9, 2015, accessed March 19, 2021, https://2014-2017.commerce.gov/news/blog/2015/11/commerce-departments-digital-economy-agenda.html. This identifies four pillars: promoting a free and open Internet worldwide; promoting trust online; ensuring access for workers, families, and companies; and promoting innovation.

[4] Philippe Amon, "Toward a New Economy of Trust" in *Revitalizing the Spirit of Bretton Woods: 50 Perspectives on the Future of the Global Economic System* (Washington, DC: Bretton Woods Committee), July 2019, accessed March 19, 2021, https://www.brettonwoods.org/BW75/compendium-release.

policies, inventory reserves, and the ability to substitute products or processing facilities. The United States should conduct regular assessments in the United States and in allied countries to determine critical supply chain resilience and trust, implement risk-based assurance measures, establish coordinated cybersecurity acquisition across government networks, and create more experts. A critical resource is semiconductor chip manufacturing, for which the vulnerability of foreign suppliers and the long lead time and cost of new production facilities requires the United States to invest in assured supply of semiconductor chips.

Chapter 5: Continuous Global Health Protection and Global Wellness

Inherent to the disruption caused by the COVID-19 pandemic are three systemic problems: (i) global leaders acted slowly to contain the spread of the virus, (ii) global health organizations reacted slowly to contain the spread of the virus, and (iii) a mixture of factors caused the delayed response, including late recognition of the threat, slow incorporation of science and data into decision making, poor political will, and inconsistent messaging to citizens regarding the nature of the threat and what precautions to take. Though nations may adopt their own strategies to enhance resilience and future planning, a more global approach to this interconnected system will be essential. The United States and its allies should lead the effort to field and test new approaches that enable the world to accelerate the detection of biothreat agents, universalize treatment methods, and deploy mass remediation, through multiple global means. This is needed not only for recovering from the COVID-19 pandemic and future outbreaks, but also for human-developed pathogens.

Chapter 6: Assured Space Operations for Public Benefit

The world is transforming from space assets being dominated almost entirely by government to being largely dominated by the private sector.[5] To maintain trusted, secure, and technically superior space operations, the United States must ensure it is a leading provider of needed space services and innovation in launch, on-board servicing, remote sensing, communications, and ground infrastructures. A robust commercial space industry not only enhances the resilience of the US national security space system by increasing space industrial base capacity, workforce, and responsiveness,

[5] Simonetta Di Pippo, "Space Technology and the Implementation of the 2030 Agenda," *UN Chronicle* 55 (4) (January 2019): 61-63, accessed April 16, 2021, https://www.un.org/en/chronicle/article/space-technology-and-implementation-2030-agenda; Matt Weinzierl and Mehak Sarang, "The Commercial Space Age Is Here," *Harvard Business Review*, February 12, 2021, accessed April 16, 2021, https://hbr.org/2021/02/the-commercial-space-age-is-here; Matt Weinzierl, "Space, the Final Economic Frontier," *Journal of Economic Perspectives* 32 (2) (Spring 2018): 173-192, accessed April 16, 2021, https://www.hbs.edu/ris/Publication%20Files/jep.32.2.173_Space,%20the%20Final%20Economic%20Frontier_413bf24d-42e6-4cea-8cc5-a0d2f6fc6a70.pdf; KPMG, *30 Voices on 2030: The future of space: Communal, commercial, contested*, May 2020, accessed April 16, 2021, https://assets.kpmg/content/dam/kpmg/au/pdf/2020/30-voices-on-2030-future-of-space.pdf.

but also advances a dynamic innovative environment that can bolster US competitiveness across existing industries, while facilitating the development of new ones. The United States should foster the development of commercial space technologies that can enhance national security space operations and improve agriculture, ocean exploration, and climate change activities, as well as align civilian and military operations and international treaties to support these uses.

Chapter 7: Future of Work

People will power the GeoTech Decade, even as technology and data capabilities transform how people live, work, and operate as societies around the world. Successful societies will be those that found ways to augment human strengths with approaches to technology and data that were uplifting, while also working to minimize biases and other shortcomings of both humans and machines. Developing a digitally resilient workforce that can meet these challenges will require private and public sectors to take an all-of-the-above approach, embracing everything from traditional educational pathways to nontraditional avenues that include employer-led apprenticeships and mid-career upskilling. Ensuring that people are not left behind by the advance of technology—and that societies have the workforces they need to innovate and prosper—will determine whether the GeoTech Decade achieves its full promise of improving security and peace.

Appendices

The remainder of the report includes the following appendices that discuss the technical foundations and potential solutions for several important challenges:

- Appendix A. Additional Readings on Identifying and Countering Online Misinformation
- Appendix B. Improving the Software Supply Chains and System Resiliency for the US Government
- Appendix C. Advancing a Data Fabric for Achieving Continuous Global Health Protection
- Appendix D. Additional Readings on the History and Future of Global Space Governance
- Appendix E. Informational GeoTech Center Synopses

Table 1. Summary of the GeoTech Commission's Findings and Recommendations

	Findings	Recommendations
1. Global science and technology leadership	The US National Strategy for Critical and Emerging Technologies requires an implementation plan to guide both domestic and international coordination to achieve global science and technology leadership.	Establish priorities, investments, standards, and rules for technology dissemination; develop across government, private industry, academia, and with allies and partners.
2. Secure data and communications	Expanding cybersecurity vulnerabilities require partnerships between the public and private sectors. Long-term quantum information science priorities include international collaboration, which is limited by national and regional funding and data sharing policies.	The United States should update and renew the National Cyber Strategy's Implementation Plan with a focus on streamlining how public and private sector entities monitor their digital environments. With allies and partners, the United States should develop priority global initiatives that employ transformative quantum information science and catalyze the development of human capital and infrastructure for these and other next-generation quantum information science applications.
3. Enhanced trust and confidence in the digital economy	To enhance trust and confidence in artificial intelligence and other digital capabilities, technologies must objectively meet the public's needs for privacy, security, transparency, and accountability.	Develop international standards and best practices for a trusted digital economy that accommodate national rules and regulations, streamline the process of independently assessing adherence to these standards.
4. Assured supply chains and system resiliency	Resilient, trusted supply chains require defense, diversification, and reinvention.	Conduct regularized assessments in the United States and in allied countries to determine critical supply chain resilience and trust, implement risk-based assurance measures. Establish coordinated cybersecurity acquisition across government networks and create more experts.
5. Continuous global health protection and global wellness	There is a need for a continuous biological surveillance, detection, and prevention capability.	Field and test new approaches that enable the world to accelerate the detection of biothreat agents, to universalize treatment methods, and to engage in mass remediation, through multiple global means.
6. Assured space operations for public benefit	The US commercial space industry can increase its role in supporting national security.	Foster the development of commercial space technologies and develop a cross-agency strategy and approach to space that can enhance national security space operations and improve agriculture, ocean exploration, and climate change activities; align both civilian and military operations, and international treaties to support these uses.
7. Future of Work	Create the workforce for the GeoTech Decade, and equitable access to opportunity	

Table 2. List of All Recommendations of the Commission in Abridged Form

	Strategy	Governance & Leadership	Capabilities	International Allies
1. Global science and technology leadership	1.1 Develop National & Economic Security Technology Strategy	1.2 Establish Global GeoTech Alliance	1.4 Review nations' use of technology with focus on privacy, civil liberties, rights 1.5 Assess risks of technology applications ability to violate rights	1.3 Strengthen S&T collaboration 1.6 Establish training, education programs to foster technology leadership
2. Secure data and communications	2A.1 Strengthen National Cyber Strategy Implementation Plan 2B.2 Conduct QIS R&D focused on digital economy issues	2A.3 Bolster compliance with NIST guidance for continuous monitoring 2A.4 Ensure cybersecurity expertise, testing are widely available	2A.2 Coordinate gov't H/W, S/W monitoring 2B.3 Accelerate QIS technologies operationalization 2B.5 Establish national QIS infrastructure	2B.1 Establish shared quantum data and communications security milestones 2B.4 Set international data/ communications standards
3. Enhanced trust and confidence in the digital economy	3.5 Assess digital infrastructure trustworthiness standards 3.6 Educate public on trustworthy digital information	3.1 Develop a US data privacy standard 3.4 Empower an organization to audit trust in the digital economy	3.3 Create measures and standards for digital economy trust 3.7 Demonstrate AI improvements to delivery of public- and private-sector services	3.2 Develop privacy-preserving technologies for the digital economy 3.8 Produce AI ethical, social, trust and governance assessment framework
4. Assured supply chains and system resiliency	4.3 Develop a geopolitical cyber deterrence strategy for critical digital resources	4.2 Broaden federal oversight of supply chain assurance	4.1 Identify and collect critical resource data	4.4 Assess physical and software/IT supply chain with allies
5. Continuous global health protection and global wellness	5.1 Launch a global pandemic surveillance and warning system	5.2 Reestablish extant pandemic monitoring 5.3 Prioritize privacy protections in pandemic surveillance	5.5 Develop vaccine, therapeutics capacity for discovery, development, distribution 5.6 Develop rapid responses to unknown pathogens	5.4 Increase medical supply chain resilience
6. Assured space operations for public benefit	6.1 Foster public benefits via federal space investments	6.3 Harden security of commercial space industry facilities and space assets	6.2 Foster and protect strategic space tech 6.5 Develop technologies for mega-constellation monitoring satellites	6.4 Establish conformance of commercial space systems to multinational agreements
7. Future of work	Create the Workforce for the GeoTech Decade, and Equitable Access to Opportunity			

Chapter 1. Global Science and Technology Leadership

A lab technician loading a semiconductor DNA sequencing chip used to identify specific cancer mutations in an individual. A crucial component of science and technology leadership is rapidly training individuals and companies to employed advanced technology capabilities. Photo taken at the Advanced Technology Research Facility (ATRF) at the Frederick National Laboratory for Cancer Research, National Cancer Institute.

NATIONAL CANCER INSTITUTE VIA UNSPLASH

The United States and like-minded nations, as well as private sector organizations, must continue to invest in and develop the multilateral mechanisms and academic and industrial capabilities, and the human capital needed for continued leadership in key science and technology (S&T) areas. Such leadership is essential for national and economic security and for ensuring that technology is developed and deployed with democratic values and standards in mind. The global development of advanced technologies requires the United States to pursue, as strategic goals and in collaboration with allies and partners, leadership in select areas.[6]

Six broad areas of S&T are critical to national and economic security, as follows:[7]

[6] Democracy Technology Partnership Act, S. 604 — 117th Congress (2021-2022), 1st Session, accessed March 19, 2021, https://www.warner.senate.gov/public/_cache/files/c/9/c9502023-85b4-4f7d-90db-9045237da704/18C2CE128388C4EC06C87EE8E4CEFB76.democracy-technology-partnership-act-bill-text.pdf.

[7] President's Council of Advisors on Science and Technology, *Recommendations for Strengthening American Leadership in Industries of the Future. A Report to the President of the United States of America*, June 2020, https://science.osti.gov/-/media/_/pdf/about/pcast/202006/PCAST_June_2020_Report.pdf?la=en&hash=019A4F17C79FDEE5005C51D3D6CAC81FB31E3ABC; White House, "National Strategy for Critical and Emerging Technologies," October 2020, accessed March 19, 2021, https://sesecuritycenter.org/national-strategy-for-critical-and-emerging-technologies/.

- **Communications and networking, data science, and cloud computing:** collectively provide the foundation for secure transmission of data for both the public and private sector and enable robust economies of ideas, resources, and talent. This critical area supports all aspects of a healthy digital economy domestically and internationally.
- **Artificial intelligence (AI), distributed sensors, edge computing, and the Internet of Things (IoT):** add new capabilities for understanding changes in the world for both physical and digital environments and enhance human governance in key, defined areas.
- **Biotechnologies, precision medicine, and genomic technologies:** collectively provide the foundation to heal and promote healthy individuals and communities, as well as to improve the performance of agricultural systems with regard to the reduction of atmospheric greenhouse gases, and to develop a system for early warning of emerging natural and human-produced risks such as outbreaks, bioterrorism, and environmental shocks.
- **Space technologies, undersea technologies, and new materials for extreme environments:** collectively provide for commercial companies and nations around the world to deploy mega-constellations of satellites, or fleets of autonomous ocean platforms, with advanced, persistent surveillance and communications capabilities to monitor the planet, including its oceans and environment, for emerging risks.[8]
- **Autonomous systems, robotics, and decentralized energy methods:** collectively provide the foundation to do work in dangerous or hazardous environments without risk to human lives, while at the same time augmenting human teams, potentially prompting long-term dislocations in national workforces, and requiring additional workforce talent for new technology areas.
- **Quantum information science (QIS), nanotechnology, and advanced microelectronics:** collectively provide the foundation for solving classes of computational problems, next-generation manufacturing, new ways to monitor the trustworthiness of digital and physical supply chains, as well as potentially presenting new challenges to communications security that underpin effective governance and robust economies.

Participation by industry, academia, government labs, and US allies and partners will help ensure a fast pace of discovery and innovation. Achieving global S&T leadership also requires protecting intellectual property and proprietary information, and guiding

[8] National Aeronautics and Space Administration, “Space Technology Grand Challenges,” December 2, 2010, accessed March 24, 2021, https://www.nasa.gov/pdf/503466main_space_tech_grand_challenges_12_02_10.pdf.

technology sharing with other nations based on their adherence to shared standards and values for security and privacy.

Technology sharing with non-allied nations poses strategic risks. For example, sharing advanced findings and applications of AI may benefit one nation at the expense of the other—AI-based image understanding algorithms could enhance remote sensing of military activities by commercial satellites. In other cases, new capabilities may benefit all nations, for example, a better disease testing technology.

Finding 1: The US National Strategy for Critical and Emerging Technologies requires an implementation plan to guide both domestic and international coordination to achieve global science and technology leadership.

The National Strategy for Critical and Emerging Technologies supports US national and economic security by promoting the National Security Innovation Base and by protecting the United States' technological advantage. Priority actions include developing the S&T workforce, establishing technology norms and standards that reflect democratic values and interests, ensuring research and development (R&D) funding of priorities, building strong partnerships with the private sector and with like-minded nations, and protecting the security of the technologies, their development, and how they are shared.[9] A detailed implementation plan, coordinated across the US government, is needed.[10]

Finding 1.1: Achieving and sustaining technology leadership must be a long-term national priority.

To achieve the long-term goals of technology leadership in key areas, a close and continuing interaction between S&T development and national security policy is essential.

The National Strategy for Critical and Emerging Technologies must be accompanied by long-term S&T goals resulting in demonstrations of significant import, and detailed programmatic plans for achieving these goals. The breadth of these technologies and their interdependencies require that progress should be shared with allies and partners and involve public-private partnerships (PPPs) among government research centers, private industry, and academia. This approach can catalyze human capital development and accelerate innovation.

[9] White House, "National Strategy," 7-9.

[10] US Government Accountability Office, *DoD Critical Technologies: Plans for Communicating, Assessing, and Overseeing Protection Efforts Should Be Completed*, GAO-21-158, January 2021, accessed April 16, 2021, https://www.gao.gov/assets/gao-21-158.pdf.

Finding 1.2: Private sector research and development exceeds that of the government in some areas that are important for national and economic security, underscoring the need for greater coordination.

The annual growth rate of domestic R&D government spending for 2000-2017 places the United States sixth, at 4.3 percent, behind the European Union (EU), Germany, India, South Korea, and China (17.3 percent).[11] The US government funds the largest share of basic research, while US industry funds the largest share of both applied research and development.[12]

Among the more important critical and emerging technologies are AI, quantum, cyber, digital infrastructure, and health/medical technologies, all areas in which private industry is growing. To strengthen US technology leadership, the United States must increase government R&D funding in critical areas and coordinate government and private industry R&D strategies.

Finding 1.3: Recent proposed legislation addresses policies for guiding permissible technology development and use.

Several countries are developing legislation to strengthen ethical practices underpinning data collection for AI algorithms, protect data privacy, and govern data rights.[13]

"Executive Order 13960 of December 3, 2020: Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government" establishes a set of principles governing the development and use of AI.[14]

A small sampling from recent, proposed US legislation includes the following ideas:

- Require assessments of the impacts of automated decision-making systems, including AI systems. These assessments would evaluate their accuracy, bias,

[11] National Science Foundation, "The State of U.S. Science and Engineering 2020," January 2020, accessed March 24, 2021, https://ncses.nsf.gov/pubs/nsb20201/global-r-d.

[12] Congressional Research Service, "U.S. Research and Development Funding and Performance: Fact Sheet," updated January 24, 2020, accessed March 26, 2021, https://fas.org/sgp/crs/misc/R44307.pdf; the National Academies defines federal S&T as essentially comprising funding categories 6.1 and 6.2. R&D is described as being more focused on application and development. Generally, government-funded S&T is dominated by academia and R&D is dominated by industry funding. For government-focused missions (e.g., NASA or DoD), the government funds industry directly for their R&D (either through contracts or independent R&D that is an allowable cost in contracts). This amount of R&D is still less than nongovernment industry R&D.

[13] Law Library of the Library of Congress, *Regulation of Artificial Intelligence in Selected Jurisdictions*, January 2019, accessed March 26, 2021, https://www.loc.gov/law/help/artificial-intelligence/regulation-artificial-intelligence.pdf.

[14] "Executive Order 13960 of December 3, 2020: Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government," *Federal Register*, accessed March 26, 2021, https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government.

discrimination, privacy, and security.[15]

- Recommend approaches that promote the development and use of AI "while protecting civil liberties, civil rights, and economic and national security."[16]
- Reinforce government regulations for protecting the privacy rights of individuals in terms of how data are collected, protected, used, and shared.
- Establish standards governing the responsible use of data and emerging technologies that include prohibitions on the use of personal data and emerging technologies in a manner that discriminates based on protected classes.

The European Commission established a High-Level Expert Group on Artificial Intelligence that published *Ethics Guidelines for Trustworthy AI* in April 2019. These guidelines address human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, nondiscrimination and fairness, societal and environmental well-being, and accountability.[17]

The newness of the technologies and their continuing evolution challenges the creation of internationally accepted, harmonized, and tested rules. In areas such as data privacy, harmonization of standards will require a heightening of US standards. In other areas of Internet and technology governance, the United States must have a leadership role in determining international standards and rules.

Finding 1.4: Models for gaining technological leadership encourage innovation, focus on challenges concerning security or economic growth, organize governance, and draw from the global talent pool.

A recent analysis, *Innovation Policies in the United States*,[18] discusses how these policies have changed over time, citing five models: "(i) Connected, challenge model, driven by societal challenges during World War II, where innovations are rapidly turned into capabilities, (ii) Basic science-focused, disconnected, decentralized model—the linear model during the Cold War, (iii) 'Right-left' translation model wherein the desired technologies motivate the basic science, (iv) Spanning the 'valley of death' model in which government initiatives helped bridge from basic research to the use of the innovations

[15] Algorithmic Accountability Act of 2019, S. 1108 — 116th Congress (2019-2020), 1st Session, accessed March 26, 2021, https://www.congress.gov/116/bills/s1108/BILLS-116s1108is.pdf.

[16] AI in Government Act of 2020, H.R. 2575 — 116th Congress (2019-2020), accessed April 16, 2021, https://www.congress.gov/bill/116th-congress/house-bill/2575/text.

[17] European Commission, "On Artificial Intelligence - A European approach to excellence and trust," White Paper, Brussels, 19.2.2020, COM(2020) 65 final, accessed March 26, 2021, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[18] Bhavya Lal, "Innovation Policies in the United States," Science and Technology Policy Institute, Institute for Defense Analyses, Washington, DC, accessed March 26, 2021, https://gsdm.u-tokyo.ac.jp/file/170208_S2P2_Lal.pdf.

by industry, (v) Connected model in which societal needs connect innovation with the production of desired products." The analysis concludes that "basic research must be complemented with additional institutional elements that reach much further down the innovation pipeline to development and later innovation stages."

Proposed legislation introduced in the 116th Congress concerning AI research focused on convening "technical experts across academia, government, and industry to develop a detailed plan for how the United States can build, deploy, govern, and sustain a national AI research cloud."[19] Another model for research collaboration was included in proposed legislation which would "organize a coordinated national strategy for developing AI, establish and support collaborative ventures or consortia with public or private sector entities, and accelerate the responsible delivery of AI applications from government agencies, academia, and the private sector."[20] Both of these bills became law in Division E of the National Defense Authorization Act (NDAA): the Artificial Intelligence Initiative Act (Sections 5101-5105 of P.L.116-283) and the National AI Research Resource Task Force Act (Section 5106 of P.L.116-283).

The United States is a founding member of the Global Partnership on Artificial Intelligence (GPAI). "In collaboration with partners and international organizations, GPAI will bring together leading experts from industry, civil society, governments, and academia to collaborate across four Working Group themes: 1) Responsible AI; 2) Data Governance; 3) The Future of Work; and 4) Innovation & Commercialization," according to a joint statement from the GPAI's founding members.[21]

While the US model for funding R&D allows for multiple, independent lines of inquiry, in QIS, for example,[22] some coordination in international collaboration could help ensure a diversity of approaches is fostered.

[19] US Sen. Rob Portman (R-OH), Portman, Heinrich Propose National Strategy For Artificial Intelligence; Call For $2.2 Billion Investment In Education, Research & Development, press release, May 21, 2019, https://www.portman.senate.gov/newsroom/press-releases/portman-heinrich-propose-national-strategy-artificial-intelligence-call-22.

[20] US Sens. Martin Heinrich (D-NM), Rob Portman (R-OH), and Brian Schatz (D-HI), in the 116th Congress sponsored the Artificial Intelligence Initiative Act (AI-IA), S. 1558, introduced in the Senate on May 21, 2019. Artificial Intelligence Initiative Act of 2019, S. 1558 — 116th Congress (2019-2020), https://www.congress.gov/bill/116th-congress/senate-bill/1558.

[21] Department of State, "Joint Statement From Founding Members of the Global Partnership on Artificial Intelligence," June 15, 2020, accessed March 26, 2021, https://www.state.gov/joint-statement-from-founding-members-of-the-global-partnership-on-artificial-intelligence/.

[22] Subcommittee on Quantum Information Science under the Committee on Science of the National Science & Technology Council, *National Strategic Overview for Quantum Information Science*, September 2018, accessed March 26, 2021, https://www.quantum.gov/wp-content/uploads/2020/10/2018_NSTC_National_Strategic_Overview_QIS.pdf.

Approach 1: Focus the innovative work and talent on long-term capability demonstrations, while emphasizing democratic values.

The United States and like-minded nations must be successful in each of the critical technology areas, or risk a vulnerability affecting national security. Success includes investing in innovative work and talent linked to long-term capability demonstrations. A focused approach sets concrete capability goals, constructs and funds fast-paced programs, and undergoes regular review. Talent from many nations and groups will make essential contributions. In contrast with nondemocratic nations, the United States and its allies and partners possess democratic values that can empower this work.

Recommendation 1: Establish priorities, investments, standards, and rules for technology dissemination; develop across government, private industry, academia, and with allies and partners.

Recommendation 1.1: Develop a National and Economic Security Technology Strategy.

To ensure the United States and its allies remain at the forefront of strategic S&T areas, the administration should develop a National and Economic Security Technology Strategy. The administration should create long-term S&T goals informed by assessments of foreign capabilities and plans. The National and Economic Security Technology Strategy should complement the National Security Strategy and draw upon the National Strategy for Critical and Emerging Technologies and other sources. The strategy should establish a long-term plan to direct government activities, incentivize private sector investments, enhance human capital, and develop capabilities in S&T that protect US national and economic security. The US Congress should conduct annual reviews of the milestone progress and budgets for these strategic S&T areas.

The strategy should also articulate a plan to establish a strategic technology ecosystem, including public-private partnerships, academia, industry, nonprofits, and others to accelerate technological development, support experimentation and pilot projects, and facilitate the application of new technologies to national and global challenges. Possible models include the Enduring Security Framework established by the National Security Agency (NSA), sector-specific consortia that include industry and academia, innovation labs that mature technology targeted at specific sectors, national laboratories developing large-scale test and evaluation infrastructure for advanced technology development, and focusing the National Science Foundation to address S&T.[23] The strategy should articulate ways to leverage not just the US workforce, but also the global talent base, while seeking to grow and retain existing highly skilled technical talent in the United States. The

[23] Endless Frontier Act, H.R. 6978 / S. 3832 — 116th Congress (2019-2020), https://www.aip.org/fyi/federal-science-bill-tracker/116th/endless-frontier-act, introduced in the 116th Congress.

strategy should outline an approach that ensures the results of the strategic technology ecosystem provide the greatest public benefit possible from government investments.

The strategy should specifically address the following technology areas, with the strategic S&T goal for each area in italics:

1. Communications and networking, data science, and cloud computing: *provide the foundation for trustworthy digital infrastructures.*
2. Artificial intelligence (AI), distributed sensors, edge computing, and the Internet of Things (IoT): *testable, tunable, and trusted AI algorithms that are robust to limited, sparse, or corrupted data and require significantly less data, power, and time compared with today.*
3. Biotechnologies, precision medicine, and genomic technologies: *field a global system for fast, automated detection, diagnoses, and discovery of treatments for emerging pathogens, bioterrorism, and other environmental shocks to the planet.*
4. Space technologies, undersea technologies, and new materials for extreme environments: *monitor the entire planet pervasively and persistently, at high resolution and communicate the information in near-real time.*
5. Autonomous systems, robotics, and decentralized energy methods: *develop coordinated protocols for testing modular systems and methods and for evaluating emergent behaviors.*
6. Quantum information science (QIS), nanotechnology, and advanced microelectronics: *establish a national QIS infrastructure comprising research, development, computational, and testing programs, facilities, and skilled personnel; accelerate the operationalization of QIS technologies.*

Recommendation 1.2: Establish a Global GeoTech Alliance and Executive Council.

To ensure coordination between the US government and private sector on key S&T issues, the administration should create a Global GeoTech Alliance and Executive Council comprised of US private sector representatives and government representatives from the National Security Council, the Intelligence Community, the Department of Defense (DoD), the Department of State, the Treasury Department, the Department of Commerce, and the Office of the United States Trade Representative. This group—the Global GeoTech Alliance and Executive Council—would advise on issues arising from emerging technologies and data capabilities, technology cooperation, and technology standard-setting efforts, such as those raised in this report, and could provide the existing President's Intelligence Advisory Board with augmented membership and a honed focus on GeoTech issues of concern across sectors globally.

Recommendation 1.3: Strengthen international collaboration on science and technology.

The administration should develop a strategy and a new multilateral mechanism among like-minded and democratic countries to coordinate technology policy, standards, and development. This strategy should seek to coordinate strategic S&T goals and milestones for collaborations with US allies and partner nations and develop agreements for sharing information, data, and research results. The strategy should also establish a framework for facilitating technical and programmatic information exchanges, with the goal of identifying opportunities for collaboration on specific S&T projects.

The administration should also increase participation by the United States in the GPAI.[24] The *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* directs the United States to establish several national AI programs and organizations to "ensure continued US leadership in artificial intelligence and to lead the world in the development and use of trustworthy artificial intelligence systems in the public and private sectors."[25] This requires the United States to take a more active role in the GPAI—in GPAI leadership activities, AI strategy development multi-stakeholder experts group, and in the formulation and execution of the research agenda that supports the work of the multi-stakeholder experts group. Interfacing with the EU in support of the new seven-year Horizon Europe S&T initiative is another potential type of collaboration.

Recommendation 1.4: Conduct annual reviews on how nations use technology—with a focus on privacy, civil liberties, and human rights; use the findings to guide international cooperation.

The administration should conduct an annual review that assesses the extent to which other nations use or develop S&T in ways that infringe upon the privacy, civil liberties, and human rights of their citizens, and undermine global peace and security. The results of the reviews should be used to help the United States prioritize cooperative efforts and facilitate coordination on S&T activities with other nations whose application of technology promotes peace, protects human rights, upholds the rule of law, and benefits global society. There is a recent proposal, for example, by the European Commission for a joint US-EU trade council.[26] This could be one of the focal points of this approach.

[24] "The Global Partnership on Artificial Intelligence," website homepage accessed on March 26, 2021, https://www.gpai.ai/.

[25] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 117th Congress (2021-2022), Public Law No. 116-283, https://www.congress.gov/bill/116th-congress/house-bill/6395.

[26] European Commission, EU-US: A new transatlantic agenda for global change, press release, December 2, 2020, Brussels, accessed March 26, 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2279.

Recommendation 1.5: Develop risk assessments of the ability of technology applications to violate civil rights, human rights, or undermine security.

The administration should develop risk assessments[27] for technology applications to determine the potential of a technology application to violate human rights and civil liberties or to undermine security. The assessments also should identify ways to lessen the identified risks. The administration should develop an interagency process, involving the Department of Commerce, the DoD, the Department of State, the Office of the Director of National Intelligence, the Office of Science and Technology Policy, the National Institute of Standards and Technology, and the attorney general,[28] to carry out these risk assessments. The processes, criteria, and metrics should be open, transparent, and consistent with relevant US trade and export and import control laws.

Recommendation 1.6: Establish national-scale training and education programs to foster continuing technological leadership.

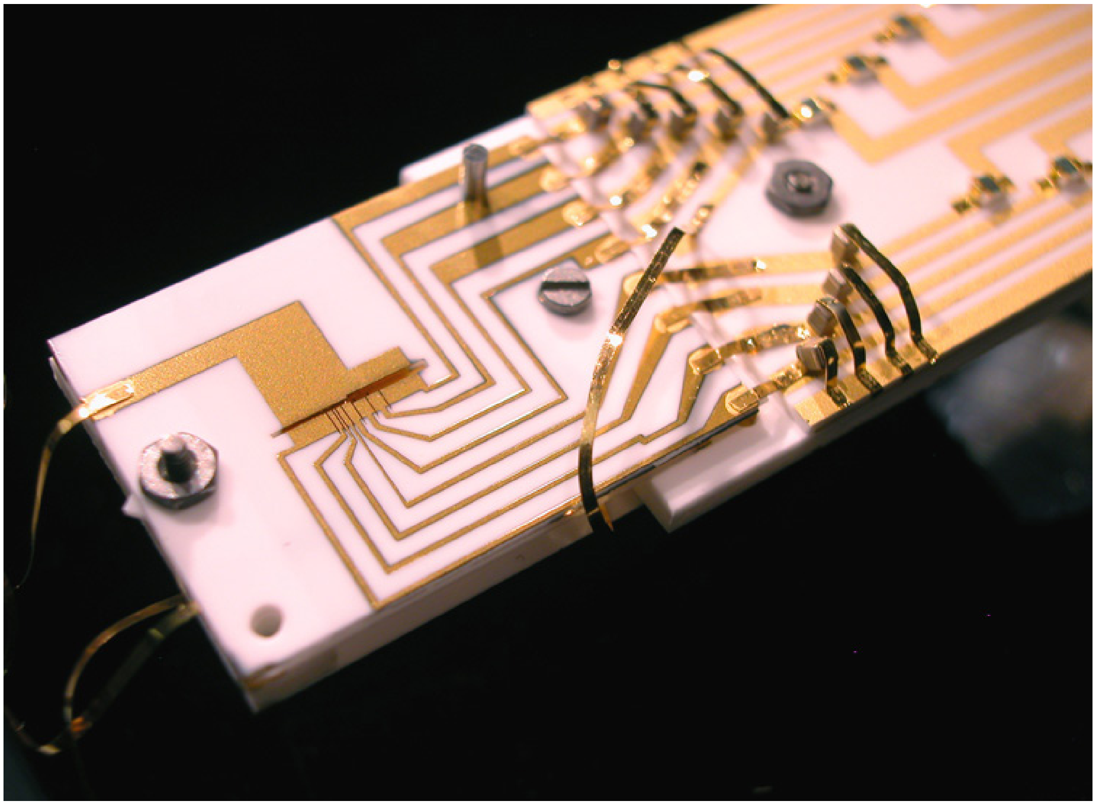
The administration should establish national-scale training and education programs to foster continuing technological leadership and to gain the strategic competitive advantage of being able to put advanced technologies to work quickly. The Department of Labor should establish a program that speeds up the matching of people to needed skills and rapidly trains individuals and companies in how to employ advanced technology capabilities. Current training methods cannot handle the fast-changing needs and numbers of students, and new mixtures of methods will evolve.[29] To help society participate in deciding how new technologies are developed and used, the administration should establish a national-scale educational program to inform the public about the benefits, risks, and brittleness of critical and emerging technologies.

[27] Asena Baykal and Thorsten Benner, *Risky Business, Rethinking Research Cooperation and Exchange with Non-Democracies, Strategies for Foundations, Universities, Civil Society Organizations, and Think Tanks*, Global Public Policy Institute, October 2020, accessed March 26, 2021, https://www.gppi.net/media/GPPi_Baykal_Benner_2020_Risky_Business_final.pdf.

[28] Bureau of Industry and Security, "Scope of Export Administration Regulations, Part 734," Department of Commerce, accessed March 26, 2021, https://www.bis.doc.gov/index.php/documents/regulations-docs/2382-part-734-scope-of-the-export-administration-regulations-1/file.

[29] Lee Rainie and Janna Anderson, "The Future of Jobs and Jobs Training," Pew Research Center, May 3, 2017, accessed March 26, 2021, https://www.pewresearch.org/internet/2017/05/03/the-future-of-jobs-and-jobs-training/.

Chapter 2. Secure Data and Communications



NIST physicists demonstrated sustained, reliable quantum information processing in the ion trap at the left center of this photograph, improving prospects for building a practical quantum computer

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, PUBLIC DOMAIN, VIA WIKIMEDIA COMMONS

This chapter addresses secure data and communications in two timeframes. Part A discusses current cybersecurity concerns and includes recommendations for improving US cybersecurity against an expanding range of vulnerabilities. Part B focuses on quantum information science (QIS) and recommends steps for ensuring the United States, along with its allies and partners, remains a leader in the development and operationalization of QIS technologies.

PART A: CURRENT CYBERSECURITY CONCERNS

Secure data and communications are fundamental to the United States' digital infrastructure and to attaining the full benefits of the global digital economy. Through the use of standards, risk assessments, monitoring, and technologies, the US government enables the public and private sectors to secure systems, data, and communications.

As the digital economy connects more public and private sector processes, effective cybersecurity for the US government faces several challenges: (i) the US government, through regulations, can affect though not assure the cybersecurity preparedness of the private sector; (ii) the ultimate size of the needed cybersecurity workforce to secure US government and private sector networks requires the private sector to fulfill the larger share, though some small- and medium-sized companies cannot afford a dedicated cybersecurity workforce; and (iii) US government agencies and laws for ensuring cybersecurity are not fully adapted to the evolving characteristics of cyberattacks. The effects of these limitations will lead to more attack vectors, missed early warning indicators, and lower cybersecurity preparedness. To maintain secure data and communications, the United States must overcome these limitations and must also stay ahead of adversaries' exploitation of US network and endpoint vulnerabilities.

Finding 2A: Expanding cybersecurity vulnerabilities require partnerships between the public and private sectors.

Cybersecurity vulnerabilities are increasing in scope and effect: greater connectivity yields more vectors for attacks, interdependent networks produce cascading effects, data breaches and records exposed are increasing,[30] and disjointed governance limits awareness and speed of action.

Cyberattackers leverage the interdependent parts of digital infrastructure to create complex attacks for the purposes of "coercion, sabotage, espionage, or extortion."[31] The greater number of connected devices can give attackers new, less defended points of access to systems and networks; for example, attackers could access the network controller devices in an electrical power network.[32] Software supply chains also present new cyberattack vulnerabilities when companies fail to employ industry-best security practices.

- In the recent SolarWinds Orion software supply chain attack, malware was inserted into a trusted software update, which led to significant breaches of government and private networks as the update was downloaded by as many as eighteen thousand SolarWinds customers (including other software and IT vendors). Such exploits of software/IT supply chains require knowledge of software configurations and dependencies. If a software vendor in the supply chain

[30] Joseph Johnson, "Annual number of data breaches and exposed records in the United States from 2005 to 2020," Statista, March 3, 2021, accessed April 16, 2021, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/; Joseph Johnson, "Number of data breaches in the United States from 2013 to 2019, by industry," Statista, March 9, 2021, https://www.statista.com/statistics/273572/number-of-data-breaches-in-the-united-states-by-business/.

[31] U.S. Cyberspace Solarium Commission, *United States of America Cyberspace Solarium Commission Report*, March 2020, accessed March 26, 2021, https://www.solarium.gov/report.

[32] Mission Support Center, "*Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector: Mission Support Center Analysis Report*, Idaho National Laboratory, August 2016, accessed March 26, 2021, https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf.

is vulnerable, then its software updates become vectors for diffusing malware.[33]

Interdependencies among networks, including between digital infrastructures and physical systems or people, are a growing type of vulnerability. Three cases illustrate such interdependencies. In a cyber risk assessment of the election infrastructure, the Cybersecurity and Infrastructure Security Agency (CISA) found that "Disinformation campaigns conducted in concert with cyberattacks on election infrastructure can amplify disruptions of electoral processes and public distrust of election results."[34] Ransomware attacks cost institutions money, caused inconvenience, and disrupted the healthcare at some hospitals.[35] An adversary could hold hostage one of the US critical infrastructure sectors[36] to preempt US military or diplomatic responses.

Data are as important as the networks, and are the foundation for new capabilities to monitor the climate, global health, agriculture, and cyberspace. Large data collections are essential for new applications of AI and innovations in medicine and education. The data infrastructure, including where the data are stored, analyzed, and the networks that communicate the results, are targets for cyberattacks.

Advanced cyberattacks take advantage of the limited information sharing between government cybersecurity experts and private industry, and the limited collection of cyberattack indicator information on private systems. Cyberattackers can spend weeks or months carefully probing the target systems, unnoticed.

Federal and private sector organizations lack sufficient insight into system operations, acquired software dependencies, and vendor practices. Also lacking is an effective system of liability and incentives to promote software supply chain security.

Finding 2A.1: Private sector infrastructure critical for economic or national security needs strengthened cybersecurity.

Private sector enterprises and small businesses can be a vector for significant attacks on critical infrastructure, yet cannot readily access or benefit from US government

[33] Ken Thompson, "Reflections on Trusting Trust," *Communications of the ACM*, Volume 27 (8) (August 1984): 761-763, accessed March 26, 2021, https://www.cs.cmu.edu/~rdriley/487/papers/Thompson_1984_ReflectionsonTrustingTrust.pdf.

[34] Cybersecurity and Infrastructure Security Agency, "Election Infrastructure Cyber Risk Assessment," Critical Infrastructure Security and Resilience Note, July 28, 2020, accessed March 26, 2021, https://www.cisa.gov/sites/default/files/publications/cisa-election-infrastructure-cyber-risk-assessment_508.pdf.

[35] Internet Crime Complaint Center, *Internet Crime Report 2020*, Federal Bureau of Investigation, accessed March 26, 2021, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

[36] White House, President Barack Obama, "Presidential Policy Directive – Critical Infrastructure Security and Resilience, PPD-21," February 12, 2013, accessed March 26, 2021, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

cybersecurity expertise. According to *Securing Cyber Assets, Addressing Urgent Cyber Threats to Critical Infrastructure*:[37]

"[M]any outstanding federal capabilities play crucial roles in cyber defense and resilience today. However, their effectiveness is constrained in the following ways:

- Private sector knowledge of these [federal cybersecurity] capabilities and incentives to use them is limited.
- Access [to federal cybersecurity capabilities] is hindered by multiple legal and administrative constraints.
- Government capabilities are scattered across a wide swath of agencies, departments, and their sub-units—a complicated labyrinth comparatively few can effectively navigate.
- Classification of essential threat information can delay and hinder coordinated response."

The following sources of cyber information and resources, along with improved coordination with the federal government, can address these needs: (i) Government sharing of critical information about cyberthreats, capabilities, and early attack indicators. This information can help private companies focus their cyberdefense resources and be more agile in doing so. (ii) A national cyber strategy that incorporates the private sector as an integral participant. This requires clarifying the laws governing the ability of the US government to direct the cybersecurity actions of private sector entities, including obligatory information sharing from certain private sector entities. (iii) For software/IT supply chains that support critical economic or national security infrastructure, US government provided risk information on vendors and components flowing into the software/IT supply chain, based on comprehensive and up-to-date collection of supply chain data and analysis of supply chain risks. Private industry can use this information to inform their risk assessments. (iv) US government incentives that assist private industry to grow the cybersecurity workforce needed to make the private sector more secure.

Finding 2A.2: Obtaining the needed cybersecurity workforce and expertise requires participation by the public and the private sector.

"Executive Order 13870 of May 2, 2019: America's Cybersecurity Workforce,"[38] estab-

[37] The President's National Infrastructure Advisory Council, *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*, August 2017, accessed March 26, 2021, https://www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf.

[38] "Executive Order 13870 of May 2, 2019: America's Cybersecurity Workforce," *Federal Register*, accessed March 26, 2021, https://www.federalregister.gov/documents/2019/05/09/2019-09750/americas-cybersecurity-workforce.

lishes national requirements to expand both the federal cybersecurity workforce and the cybersecurity workforce for state, territorial, local, and tribal governments, academia, private sector stakeholders, and others. There are five hundred and twenty-one thousand unfilled cybersecurity jobs in the United States, of which thirty-seven thousand are in the federal government.[39]

The EO supports workforce mobility between the public and private sector for cybersecurity workers, and directs departments to share recruitment strategies and tools across these sectors. A starting point, for both sectors, is the Workforce Framework for Cybersecurity [National Initiative for Cybersecurity Education (NICE) Framework].[40] This defines categories and specialty areas, knowledge, tasks, skills, abilities, and work roles. It can be used by public and private sector employers to better match candidates with sets of needed skills.

To close the workforce gap in nonfederal positions, a flexible approach, consistent with the NICE Framework, may be effective.[41] The strategy is to develop new career models that are better matched to the pool of candidates, aligned with the NICE Framework where possible, and using employee development programs and financial incentives to grow workforce skills.

Finding 2A.3: Cybersecurity governance, which must enable timely protective actions, has not matched the speed of the cyber threat environment.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework comprises five functions: Identify, Protect, Detect, Respond, and Recover.[42] In each function, timely action is essential for effective cybersecurity. Yet, defensive cybersecurity posture is systemically outpaced by offensive actors.

- Patching quickly is imperative. A FireEye study[43] reports the average time disclosure and patch availability was approximately nine days. Other

[39] "Cybersecurity Supply/Demand Heat Map," Cyberseek.org, accessed March 26, 2021, https://www.cyberseek.org/heatmap.html.

[40] National Initiative for Cybersecurity Careers and Studies, "Workforce Framework for Cybersecurity (NICE Framework)," Cybersecurity and Infrastructure Security Agency, accessed March 26, 2021, https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework.

[41] Aspen Institute, *Principles for Growing and Sustaining the Nation's Cybersecurity Workforce*, November 2018, accessed March 26, 2021, https://www.aspeninstitute.org/wp-content/uploads/2018/11/Aspen-Cybersecurity-Group-Principles-for-Growing-and-Sustaining-the-Nations-Cybersecurity-Workforce-1.pdf.

[42] "Cybersecurity Framework," National Institute of Standards and Technology, accessed March 26, 2021, https://www.nist.gov/cyberframework/online-learning/five-functions.

[43] Kathleen Metrick, Jared Semrau, and Shambavi Sadayappan, "Think Fast: Time Between Disclosure, Patch Release and Vulnerability Exploitation — Intelligence for Vulnerability Management, Part Two," FireEye, April 13, 2020, accessed April 16, 2021, https://www.fireeye.com/blog/threat-research/2020/04/time-between-disclosure-patch-release-and-vulnerability-exploitation.html.

reports[44] have found longer times to patch though—up to thirty-eight days on average—and some of the most notorious cyber incidents exploited vulnerabilities patched months before their compromise.[45]

- Organizational adjustments and implementation of best practices must be rapid to keep up with developing threats. Yet, at the federal level, many agencies have been unable to adopt NIST-recommended best practices for ICT supply chain risk management for years.[46]
- Timely and rapid detection and response is necessary to forestall damage and the risk of cascading effects. This capability relies on a system of indicators and warnings, and, at times, comprehensive situational awareness that allows one to monitor cyber events closely and deploy defensive tools with precision. Still, the most sophisticated incursions can remain undetected for months.[47]
- Timely recovery depends on having built resilience into the digital infrastructure, and in having efficient decision making. Long-running attacks, however, can take more than a year to fully recover from.[48]
- All core cybersecurity functions depend on efficient information sharing between and within the public and private sectors. Yet, industry still complains about their incident response being hampered by liability concerns[49] and information sharing challenges.[50]

[44] Rapid7, "Security Report for In-Production Web Applications," White Paper, accessed April 16, 2021, https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-tcell-application-security-report.pdf.

[45] Amir Preminger, "NotPetya: Looking Back Three Years Later," Claroty, June 30, 2020, accessed April 16, 2021, https://claroty.com/2020/06/30/notpetya-looking-back-three-years-later/.

[46] United States Government Accountability Office, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-171, December 15, 2020, accessed March 26, 2021, https://www.gao.gov/assets/gao-21-171.pdf.

[47] Robert McMillan, "Hackers Lurked in SolarWinds Email System for at Least 9 Months, CEO Says," *Wall Street Journal*, February 2, 2021, accessed April 16, 2021, https://www.wsj.com/articles/hackers-lurked-in-solarwinds-email-system-for-at-least-9-months-ceo-says-11612317963.

[48] Patrick Howell O'Neill, "Recovering from SolarWinds hack could take 18 months," *MIT Technology Review*, March 2, 2021, accessed April 16, 2021, https://www.technologyreview.com/2021/03/02/1020166/solarwinds-brandon-wales-hack-recovery-18-months/.

[49] Cybersecurity and Infrastructure Security Agency, *Information and Communications Technology Supply Chain Risk Management Task Force Year 2 Report: Status Update on Activities and Objectives of the Task Force*, December 2020, accessed April 16, 2021, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force_year-two-report_508.pdf.

[50] Lauren Feiner, "Microsoft president: The only reason we know about SolarWinds hack is because FireEye told us," CNBC, February 23, 2021, accessed April 16, 2021, https://www.cnbc.com/2021/02/23/microsoft-exec-brad-smith-praises-fireeye-in-solarwinds-hack-testimony.html.

Approach 2A: Establish comprehensive situational awareness of cybersecurity risks in systems that are critical for national and economic security.

The foundation of an effective cybersecurity strategy is comprehensive situational awareness of the state of the critical infrastructure for economic and national security. This is built upon the continuous collection of key indicators, prioritization of risk, the ability to assess key points in the software/IT supply chain, standards to inform best practices, and assessments of the actual levels of cyberdefense and resilience.

To achieve such comprehensive situational awareness requires that the public and private sectors must develop a partnership that ensures sufficient information is monitored and exchanged; that the authorities for taking action, when needed, are established in law; and that sufficient cybersecurity training and knowledge is available across the private sector to help strengthen the cybersecurity of this sector.

Recommendation 2A: The United States should update and renew the National Cyber Strategy's Implementation Plan with a focus on streamlining how public and private sector entities monitor their digital environments.

Recommendation 2A.1: Review, update, and reestablish the Implementation Plan for the National Cyber Strategy.

The administration should establish a process to incorporate both regular and ad hoc updates into the National Cyber Strategy so that the strategy remains current and evolves to meet future cybersecurity threats and challenges.[51] The strategy should retain focus on streamlining how public and private sector entities continuously monitor their digital environments to include outlining the appropriate roles, responsibilities, and governance. In addition to a single national cyber coordinator[52] that was established in the FY 2021 National Defense Authorization Act (NDAA), the strategy should consider the following components: uniform rules and increased compliance with standards for cybersecurity practices across all government activities (with exceptions for national security activities); skilled cybersecurity officers either in, or embedded in, organizations; and a national educational program to improve individuals' cybersecurity habits.

[51] Government Accountability Office, *Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*, report to congressional requestors, September 2020, accessed March 26, 2021, https://www.gao.gov/assets/gao-20-629.pdf; National Security Council, National Cyber Strategy Implementation Plan (Washington, D.C.: June 2019). The Implementation Plan was not published to the public, but any entity assigned a lead or supporting role within the plan received a digital copy of the plan.

[52] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021.

Recommendation 2A.2: Establish effective and coordinated continuous monitoring for software and hardware used by the federal government.

As part of COVID-19 pandemic relief, the America Rescue Plan Act of 2021 (Public Law No: 117-2, March 11, 2021)[53] includes $1.65 billion for cybersecurity capabilities, readiness, and resilience. This increases the Technology Modernization Fund and helps CISA and the General Services Administration (GSA) complete modernization projects at federal agencies. Additional funds for CISA could bolster cybersecurity across federal civilian agency networks and support pilot programs for shared security and cloud computing services.

The acquisition strategies to achieve cybersecurity resilience should reflect the unique cybersecurity requirements and the need for specialized expertise in operations and networks supporting Title 5 (Government Organization and Employees), Title 10 (Armed Forces), Title 34 (Crime Control and Law Enforcement), and Title 50 (War and National Defense) of the US Code. The acquisition strategies should strengthen compliance with standards for continuous monitoring of cybersecurity performance.

The federal government should seek to achieve continuous cybersecurity monitoring of the hardware and software systems that support US government functions, including critical supply chains and network infrastructure. The approach should ensure coordination across all relevant elements of the federal government. Attributes to monitor include external network traffic, internal network behavior, vulnerability exposure, asset tracking, security posture, vendor compliance, product compliance, and product updates. There are four contributing activities to fully realize a cybersecurity posture informed by continuous monitoring: (i) assess the trustworthiness of software and hardware employed by the US government based on inherent vulnerabilities and risks due to the network position, permissions, and supply chain considerations; (ii) further empower the Department of Homeland Security (DHS) to perform these assessments by strengthening the ties among US government agency chief information officers (CIOs) and DHS for the various government networks; (iii) make these hardware and software risk assessments available to local and state governments to inform their endeavors; and (iv) leverage these assessments to support the private sector, especially small- to mid-sized businesses that do not have the capacity to fully assess their own supply chains yet would benefit from knowing what software is trustworthy. The risk assessments developed by the US government could also be shared with like-minded partners that are seeking to do the same regarding the hardware and software they employ to achieve assured supply chains and trusted digital environments.

There are several lines of effort, described further in Appendix B.

[53] American Rescue Plan Act of 2021, H.R. 1319, Public Law No. 117-2, 117th Congress (2021-2022), https://www.congress.gov/bill/117th-congress/house-bill/1319/text.

Recommendation 2A.3: Increase compliance with continuous monitoring that is part of the National Institute of Standards and Technology security control guidance.

The administration should require GAO to review the efficacy of agency-specific practices regarding the continuous monitoring portion of its security control guidance. NIST controls dedicated to continuous monitoring for agencies[54] are required for all three priority levels of the federal agency information systems.[55] OMB memoranda as far back as 2011[56] discuss continuous monitoring superseding periodic reviews. While NIST has long recommended the practice, agencies have failed to implement it: in 2019, only about three-quarters had done so,[57] marking little improvement over several years. The most recent GAO report[58] indicates that general compliance with fundamental risk management practices has turned worse.

To achieve increased compliance, CISA should be empowered to assist lagging agencies in conforming with NIST guidelines and best practices mandated by the Federal Information Security Modernization Act (FISMA).[59] This would support a more responsive and uniform implementation of security methods—monitoring, security updates, approaches such as stress tests, assessing vendor security maturity, and certificate transparency. New data disclosure policies must be developed to enable the mapping, visualization, and testing of the software/IT supply chain networks.[60]

More specific understanding of the continuous monitoring practices is needed to guide implementation. There is overlap in the types of continuous monitoring discussed most often. First is the continuous monitoring of vendor compliance with certification regimes— the Federal Risk and Authorization Management Program (FedRAMP), the

[54] "NIST Risk Management Framework," National Institute of Standards and Technology Computer Security Resource Center, accessed March 26, 2021, https://nvd.nist.gov/800-53/Rev4/control/CA-7.

[55] Kelley Dempsey et al., *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, Special Publication 800-137, NIST, September 2011, accessed March 26, 2021, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf.

[56] Office of Management and Budget, "FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," Executive Office of the President, Memorandum M-11-33, September 14, 2011, accessed March 26, 2021, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-33.pdf.

[57] Executive Office of the President of the United States, *Federal Information Security Modernization Act of 2014: Annual Report to Congress, Fiscal Year 2019*, accessed March 26, 2021, https://www.whitehouse.gov/wp-content/uploads/2020/05/2019-FISMARMAs.pdf.

[58] Government Accountability Office, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-171, December 15, 2020, accessed March 26, 2021, https://www.gao.gov/products/GAO-21-171.

[59] *Federal Information Security Modernization Act of 2014*, S. 2521 — 113th Congress (2013-2014), https://www.congress.gov/bill/113th-congress/senate-bill/2521/text; FISMA requires each agency to handle its own security by meeting NIST SP 800-53 controls as well as requiring their information systems maintainers to comply with NIST SP 800-171. These NIST publications discuss continuous monitoring controls, with NIST SP 800-137 dedicated to even more, in depth consideration.

[60] Cybersecurity and Infrastructure Security Agency, *Information and Communications Technology*.

Department of Defense (DoD) information networks approved product list (DoDIN APL), the new *Cybersecurity Maturity Model Certification (CMMC)*, etc. Each describes and aspires toward continuous assessment of compliance, but they are still organized around monthly, yearly, or three-year review periods. Truly continuous monitoring would bring more rigor and regularity to reviewing changes made to deployed software, a potentially devastating attack vector for adversaries, and changes in vendor security practices and context.

NIST guidelines refer to continuous monitoring of security control efficacy, asset exposure, threat vulnerability, configuration compliance, and other quasi-technical metrics. Between 79 percent and 83 percent of Chief Financial Officers Act of 1990 (CFO Act) federal agencies,[61] and between 58 percent and 63 percent of non-CFO Act agencies, fulfill these requirements. This type of continuous monitoring is determined by agency policy, leading to varying standards for how often to perform checks, what to check, and what satisfactory levels are.[62] A program at CISA, the Continuous Diagnostics and Mitigation (CDM) program, is supposed to integrate these activities. It has met systemic implementation difficulties, however,[63] and Homeland Security Secretary Alejandro Mayorkas has sought a review of the CDM program, along with CISA's EINSTEIN program, which monitors inbound and outbound traffic on federal networks.[64] It also must overcome great variation among the networks and products that would be checked. There is little agreement and the quality of implementation is not well-known.

Finally, there is the continuous monitoring of actual network behavior. This would include mandating the maintenance of standardized access logs, auditing of those logs, monitoring inbound and outbound traffic, and all the related detailed measurements. More transparency is needed in how much such monitoring occurs within government networks, though CISA's EINSTEIN program does the work of monitoring traffic in and out of federal civilian agencies.

Recommendation 2A.4: Ensure cybersecurity best practices, expertise, and assurance testing are widely available to industry and government entities.

The administration should provide the private sector technical information on threats on a regular basis, to bolster cybersecurity. The private sector outreach would be linked to the existing Information Sharing and Analysis Centers (ISACs) for US critical

[61] Executive Office of the President of the United States, *Federal Information Security Modernization Act of 2014*.

[62] Dempsey et al., *Information Security Continuous Monitoring (ISCM)*.

[63] Congressional Research Service, *Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program*, August 2020, accessed March 26, 2021, https://www.gao.gov/assets/gao-20-598.pdf.

[64] Justin Katz, "Mayorkas calls for review of Einstein, CDM," FCW, January 19, 2021, accessed March 26, 2021, https://fcw.com/articles/2021/01/19/mayorkas-dhs-confirm-cyber.aspx.

infrastructure entities and the Information Sharing and Analysis Organizations (ISAOs) to ensure monitoring of both supply chain risks and cybersecurity performance for vital US private sector companies of all sizes.

The US national security domain requires independent certification of adherence to a set of multinational standards.[65] One approach could be to expand CMMC to all of government instead of just DoD. While the program is still facing implementation challenges,[66] it could provide useful information on general cybersecurity maturity to industry and government alike, with benefits beyond the specific vendor products. Because DoD is only just beginning to implement CMMC, as a first step the administration should conduct a feasibility assessment for an across-government approach. To improve and streamline cybersecurity requirements, the administration should assess how a government-wide implementation of CMMC would overlap with FedRAMP or any other cybersecurity requirements, and how the broadened implementation of CMMC could improve general industry cyber hygiene.

To implement cybersecurity capabilities and practices, private sector companies must acquire cleared personnel, spaces, and IT equipment. The administration should consider accelerating any necessary prerequisite steps.

PART B: QUANTUM INFORMATION SCIENCES

The United States, the European Union (EU), China, Russia, the United Kingdom, Canada, and other nations are expanding their investments in QIS, with national and regional QIS strategies and programs.[67] Recent demonstrations of quantum computers increase concerns that aspects of the technical foundation of the United States'

[65] "Cybersecurity Maturity Model Certification (CMMC) Compliance," Compliance Forge, accessed March 26, 2021, https://www.cmmc-compliance.com/.

[66] Jackson Barnett, "New bottleneck emerges in DOD's contractor cybersecurity program, concerning assessors," FEDSCOOP, April 19, 2021, accessed April 21, 2021, https://www.fedscoop.com/cmmc-bottleneck-c3pao-assessments-dod/.

[67] Subcommittee on Quantum Information Science under the Committee on Science of the National Science & Technology Council, *National Strategic Overview*; "National Quantum Initiative Advisory Committee," US Department of Energy, accessed March 26, 2021, https://science.osti.gov/About/NQIAC; QUROPE Quantum Information Processing and Communication in Europe, *Quantum Technologies Roadmap*, European Union, August 2018, accessed March 26, 2021, http://qurope.eu/h2020/qtflagship/roadmap2016; National Development and Reform Commission, "The 13th Five Year Plan for Economic and Social Development of the People's Republic of China (2016-2020)," People's Republic of China, accessed March 26, 2021, https://en.ndrc.gov.cn/newsrelease_8232/201612/P020191101481868235378.pdf; Arjun Kharpal, "In battle with U.S., China to focus on 7 'frontier' technologies from chips to brain-computer fusion," CNBC, March 5, 2021, accessed March 26, 2021, https://www.cnbc.com/2021/03/05/china-to-focus-on-frontier-tech-from-chips-to-quantum-computing.html.

digital security may be vulnerable in the foreseeable future.[68] Quantum communication and quantum key distribution (QKD) methods,[69] though, can enhance the security of the digital infrastructure. These methods may contribute to data and communications security against untrusted and corrupted hardware and also protect against the ability to make inferences about sensitive data based on access to multiple data sources containing nonsensitive data.[70]

Finding 2B: Long-term quantum information science priorities include international collaboration, which is limited by national and regional funding and data-sharing policies.

A primary element of leadership in QIS is the ability to set key standards for QIS applications. This relies on developing and deploying devices that operationalize QIS, and in working in collaboration with many nations and partners. While collaboration is identified as a national priority in the US national strategy for QIS, it should be extended beyond basic S&T activities.

Finding 2B.1: The US strategy for quantum information science emphasizes US efforts and benefits.

The *National Strategic Overview for Quantum Information Science*[71] provides a strategic approach for achieving US leadership in QIS and its applications to national and economic security. The six policy areas are as follows:

- **Choosing a science-first approach to QIS**: Strengthen the research foundation and the collaboration across disciplines. Use Grand Challenge problems as a strategic mechanism to coordinate and focus efforts.
- **Creating a future quantum-smart workforce:** Foster a QIS-skilled workforce through investments in industry, academia, and government laboratories that increase the scope of QIS research, development, and education.

[68] S. Debnath et al., "Demonstration of a small programmable quantum computer with atomic qubits," Nature 536 (2016): 63-66, accessed March 26, 2021, https://doi.org/10.1038/nature18648; Google AI Quantum and Collaborators et al., "Hartree-Fock on a superconducting qubit quantum computer," *Science* 369 (6507) (August 28 2020): 1084–1089, accessed March 26, 2021, https://doi.org/10.1126/science.abb9811; Juan Yin et al., "Entanglement-based secure quantum cryptography over 1,120 kilometres," Nature 582 (2020): 501-505, accessed March 26, 2021, https://doi.org/10.1038/s41586-020-2401-y; Vasileios Mavroeidis et al., "The Impact of Quantum Computing on Present Cryptography," *International Journal of Advanced Computer Science and Applications* 9 (3) (2018), accessed April 16, 2021, https://arxiv.org/pdf/1804.00200.pdf.

[69] "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)," National Security Agency Central Security Service, accessed March 26, 2021, https://www.nsa.gov/what-we-do/cybersecurity/quantum-key-distribution-qkd-and-quantum-cryptography-qc/.

[70] M. Fujiwara et al. "Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing," *Scientific Reports* 6, 28988 (2016), accessed March 26, 2021, https://doi.org/10.1038/srep28988.

[71] Subcommittee on Quantum Information Science under the Committee on Science of the National Science & Technology Council, *National Strategic Overview*.

- **Deepening engagement with the quantum industry:** Increase coordination among the federal government, industry, and academia to enhance awareness of needs, issues, and opportunities.
- **Providing critical infrastructure:** Encourage necessary investments, create and provide access to QIS infrastructure, and establish testbeds.
- **Maintaining national security and economic growth:** Maintain awareness of the security benefits and risks of QIS capabilities.
- **Advancing international cooperation:** Seek opportunities for international cooperation to benefit the US talent pool and raise awareness about other QIS developments.

The US strategy for QIS recognizes the sensitivities of this research, which can both enable new scientific and economic applications, and create new methods for attacking sensitive data and communications. This strategy supports international collaboration in QIS both to advance the basic research and its applications, and to ensure the United States maintains its leadership and competitiveness in QIS.[72]

- The US strategy for QIS supports international efforts in three ways: It reviews international research to maintain awareness of new results and directions, selects partnerships that will give the United States access to top-quality researchers and facilities, and shares certain public data from QIS research to help the development of standards for future QIS applications.

In addition to the US strategy for QIS, the National Quantum Initiative Act "authorized $1.2 billion in federal research and development (R&D) spending over five years, established the National Quantum Coordination Office, and called for the creation of new QIS research institutes and consortia around the country."[73] Also, the National Science Foundation (NSF) recently established three quantum research centers[74] and added the opportunity for limited supplemental funding requests to support international collaboration on basic research topics.[75]

[72] Ibid.

[73] National Quantum Initiative Act of 2018, S. 3143, Public Law No. 115-368, 115th Congress (2017-2018), accessed March 26, 2021, https://www.congress.gov/115/plaws/publ368/PLAW-115publ368.pdf.

[74] National Science Foundation, "NSF establishes 3 new institutes to address critical challenges in quantum information science," Announcement, July 21, 2020, accessed March 26, 2021, https://www.nsf.gov/news/special_reports/announcements/072120.jsp.

[75] "Dear Colleague Letter: International Collaboration Supplements in Quantum Information Science and Engineering Research," National Science Foundation, NSF 20-063, March 24, 2020, accessed March 26, 2021, https://nsf.gov/pubs/2020/nsf20063/nsf20063.jsp.

Congressional hearings on "Industries of the Future" discussed the importance of QIS and establishing US leadership in QIS.[76] One effort by the United States to establish international cooperation in QIS is the agreement between the United States and Japan to cooperate on quantum research through activities including "collaborating in venues such as workshops, seminars, and conferences to discuss and recognize the progress of research in QIST, which in turn will lead to the identification of overlapping interests and opportunities for future scientific cooperation."[77]

Finding 2B.2: China is pursuing quantum information science as a strategic technology.

Quantum communications and computing are among the strategic technologies highlighted in China's 14th Five-Year Plan (2021-2025). China aims to be a global leader in innovation, using large demonstration projects to advance its science and technology (S&T), and to build human capital for strategic technology areas. This includes major initiatives in quantum research and development (R&D), demonstrations of QKD and quantum computing, and a major new National Laboratory for Quantum Information Sciences.[78] China is able to advance in quantum R&D in part due to the close coordination among the government, universities, and industry, which aids both the advancement of the science and the building of a skilled workforce.[79]

Finding 2B.3: EU's science and technology strategy focuses on EU participation.

The EU's S&T program includes three components that address QIS and other technology areas: (i) Horizon Europe, which has a seven-year budget of €95.5 billion for 2021-2027, within which the Digital, Industry and Space area is funded at €15.5 billion;[80] (ii)

[76] "Industries of the Future," U.S. Senate Committee on Commerce, Science, and Transportation, January 15, 2020, accessed March 26, 2021, https://www.commerce.senate.gov/2020/1/industries-of-the-future.

[77] "Tokyo Statement on Quantum Cooperation," U.S. Department of State, December 19, 2019, accessed March 26, 2021, https://www.state.gov/tokyo-statement-on-quantum-cooperation/.

[78] Elsa B. Kania, "China's Quantum Future," *Foreign Affairs*, September 26, 2018, https://www.foreignaffairs.com/articles/china/2018-09-26/chinas-quantum-future; European Commission, "Quantum Technologies Flagship kicks off with first 20 projects," Factsheet, October 29, 2018, accessed March 26, 2016, https://ec.europa.eu/commission/presscorner/detail/de/MEMO_18_6241; Arjun Kharpal, "In battle with U.S., China to focus on 7 'frontier' technologies from chips to brain-computer fusion," CNBC, March 5, 2021, accessed March 26, 2021, https://www.cnbc.com/2021/03/05/china-to-focus-on-frontier-tech-from-chips-to-quantum-computing.html; Lauren Dudley, "China's Quest for Self-Reliance in the Fourteenth Five-Year Plan," *Net Politics*, March 8, 2021, accessed April 16, 2021, https://www.cfr.org/blog/chinas-quest-self-reliance-fourteenth-five-year-plan.

[79] Martin Giles, "The man turning China into a quantum superpower," *MIT Technology Review*, December 19, 2018, accessed March 26, 2021, https://www.technologyreview.com/2018/12/19/1571/the-man-turning-china-into-a-quantum-superpower/.

[80] "Final budget breakdown Horizon Europe," Science|Business, accessed April 16, 2021, https://sciencebusiness.net/sites/default/files/inline-files/Final%20budget%20breakdown%20Horizon%20Europe_0.pdf.

Digital Europe Programme, funded at €7.5 billion;[81] and (iii) Space Programme, with proposed funding of €13.2 billion.[82] The European Commission is soliciting proposals for quantum communications infrastructure, which will be funded by these initiatives. The objective is to enable the EU to be an independent provider of quantum technologies needed to build a quantum communications infrastructure.[83]

Horizon 2020, the predecessor to Horizon Europe, involved US researchers in only 1.5 percent of the Horizon 2020 projects.[84] In comparison, EU researchers participate at a much greater level considering all National Science Foundation (NSF) and National Institutes of Health (NIH) active grants.[85] This asymmetry in participation is due to EU rules that require participants in Horizon 2020 projects to sign grant agreements. For US institutions, this raises issues concerning "governing law and jurisdiction, intellectual property treatment, joint and several liability[86] and indemnification, access to data and implications for export control, and auditing requirements."[87]

Finding 2B.4: Funding policies constrain collaboration.

One issue of concern in the Horizon Europe initiative rules governing participation is the determination of financial contribution by the United States and "third countries" as defined in Article 12 of Horizon Europe—the Framework Programme for Research

[81] "Digital Europe Programme," European Commission, accessed April 16, 2021, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/digital.

[82] European Commission, Commission welcomes the political agreement on the European Space Programme, press release, December 16, 2020, accessed April 16, 2021, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2449.

[83] European Commission, "European Commission, Call for tenders CNECT/LUX/2020/CPN/0062, Detailed system study for a Quantum Communication Infrastructure, Competitive Procedure with Negotiation," accessed April 16, 2021, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69304; Éanna Kelly, "Switzerland pencilled back into quantum plans, but no access for UK, Israel," Science|Business, March 18, 2021, accessed April 16, 2021, https://sciencebusiness.net/news/switzerland-pencilled-back-quantum-plans-no-access-uk-israel; "Horizon Europe, Work Programme 2021-2022, 7. Digital, Industry and Space," European Commission, accessed April 16, 2021, https://sciencebusiness.net/sites/default/files/inline-files/7.%20Digital%20Industry%20Space.pdf.

[84] CORDIS, European Commission Research Results, accessed April 16, 2021, https://cordis.europa.eu/projects/en. This represents a comparison of Horizon 2020 projects originating in the United States during 2013-2020 with the total number of Horizon 2020 projects, excluding certain subcategories from both groupings.

[85] "Funding & tender opportunities, Single Electronic Data Interchange Area (SEDIA)," European Commission, accessed March 26, 2021, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-dashboard.

[86] "When two or more parties are jointly and severally liable for a tortious act, each party is independently liable for the full extent of the injuries stemming from the tortious act." "Joint and Several Liability," Cornell Law School, accessed March 26, 2021, https://www.law.cornell.edu/wex/joint_and_several_liability.

[87] Richard L. Hudson, "Tale of two cities: Brussels and Washington struggle to cooperate in science," Science|Business, May 14, 2018, accessed April 16, 2021, https://sciencebusiness.net/tale-two-cities-brussels-and-washington-struggle-cooperate-science; Ryan Lankton and Jennifer Ponting, "Managing Horizon 2020 Grants: the Experiences of the University of Michigan and Harvard," *NCURA Magazine*, National Council of University Research Administrators, XLVIII (1) (January/February 2016), accessed April 16, 2016, http://www.ncura.edu/portals/0/docs/srag/january%202016%20issue-weibo.pdf.

and Innovation.[88] The calculated cost of association with the Horizon Europe initiative is based on the relative size of a country's gross domestic product (GDP) compared with EU GDP. For example, the European Commission has proposed making the UK pay a proportion of the 2021-2027 research budget based on its share of EU GDP, which currently stands at 18 percent. For the United States, this corresponding value is 137 percent, yielding a required contribution of $131.4 billion.

The regulations establishing Horizon Europe contain other potential issues for US participation. These include Article 36, which gives the European Commission rights regarding transfer and licensing, and Article 49, which gives certain EU entities the right to carry out investigations and inspections.

Approach 2B: Coordinate with allies and partners to build human capital for quantum information science and overcome limitations imposed by national and regional funding and data-sharing polices.

In the ongoing competitive R&D of QIS, key determinants of success are the size, skill, and collaboration of the technology workforce spanning a number of disciplines, including those in the fields of science, technology, engineering, mathematics (STEM), and manufacturing. The United States recognizes that it "must work with international partners, even while advancing domestic investments and research strategies."[89]

Recommendation 2B: With allies and partners, the United States should develop priority global initiatives that employ transformative quantum information science and catalyze the development of human capital and infrastructure for these and other next-generation quantum information science applications.

Recommendation 2B.1: Establish, with other nations, a common set of demonstration milestones for quantum data and communications security.

The administration should extend the technological development portfolio of national investments in QIS to incorporate a common set of milestones with allies. The members of the National Science and Technology Council (NSTC) Subcommittee on Quantum Information Science should develop such milestones in coordination with representatives from collaborating nations. These are to be consonant with plans by the United States and like-minded nations to develop testbeds, demonstrations, standards, and a quantum-skilled workforce. The milestones will inform the practical applications for use

[88] "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing Horizon Europe - the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination - Common understanding," Council of the European Union, Interinstitutional File: 2018/0224(COD), accessed March 26, 2021, https://www.consilium.europa.eu/media/38902/st07942-en19.pdf.

[89] Subcommittee on Quantum Information Science under the Committee on Science of the National Science & Technology Council, *National Strategic Overview*, 12.

with near-, mid-, and long-term levels of quantum information capabilities. The EU's Horizon Europe initiative is a potential opportunity for such collaboration. The United States should also establish data sharing agreements with other nations for QIS results pertaining to shared economic and national security interests.

Recommendation 2B.2: Create a program of quantum information science research and development focused on emerging issues for digital economies.

The administration should continuously evaluate QIS progress and technologies through the White House Office of Science and Technology Policy (OSTP) and the National Academies of Sciences, Engineering, and Medicine; this could be accomplished by the creation of a standing committee such as they have done for other areas that will be long-lived. This will identify new technology directions, review QIS policies, and revisit priorities and partnerships. The evaluations should focus on entirely new quantum capabilities that can benefit digital economies, e.g., privacy and advances in biotechnology and data capabilities, open sharing of data while maintaining data privacy, principles for systems to be quantum-secure by design, digital supply chain security for both hardware and software, evolution of Internet protocols, network modernization, and other topics.

Recommendation 2B.3: Establish a program to accelerate the operationalization of quantum information science technologies.

Recognizing the need for broad and significant investment in quantum applications to focus and accelerate progress, Congress and the administration should establish a program, led by the Defense Advanced Research Projects Agency (DARPA), to accelerate the operationalization of continually evolving hybrid (classical and quantum) computing architectures. This program will mature prototype demonstrations of quantum computing, communication, sensing, and metrology technologies to yield fieldable capabilities. The program also should include elements that seek to develop a quantum-skilled workforce in the private and public sectors. Several models for such a program are seen in DARPA's long history of rapidly growing and maturing advanced technology fields, e.g., Grand Challenges for autonomous vehicles, Have Blue for stealth technologies, and AI Next for artificial intelligence.

Recommendation 2B.4: Establish leading roles for the United States in setting international standards for data and communications security as quantum information science evolves.

Building on the results obtained from NDAA FY 2021, SEC. 9414, *Study on Chinese Policies and Influence in the Development of International Standards for Emerging*

Technologies,[90] the administration should take steps to bolster the development of standards for QIS technology development and applications.[91] This will drive toward a strategy for achieving a leadership role in international quantum standards setting, sharing sensitive security-related advances with allies, responding to China's efforts to influence international standards,[92] and catalyzing private sector investments in quantum technologies. NIST is currently developing quantum resilient encryption standards for the United States.[93] The administration should direct NIST to broaden the scope of its work to develop standards for QIS technology development and applications.[94]

The administration should develop DoD and Intelligence Community policy guidance to govern the sharing of QIS findings and capabilities with allies and partners. This guidance should be developed with representation from the Department of Commerce's National Telecommunications and Information Administration (NTIA) and NSF to balance security concerns with the benefits of collaboration; address government and private industry information, both classified and proprietary; and also should include categories of information that the United States is interested in receiving from allies and partners.

Recommendation 2B.5: Establish a national QIS research, development, and testing infrastructure; fund quantum demonstration programs.

The administration should establish a national QIS research, development, and testing infrastructure. This will comprise research centers focused on quantum computing, quantum communications, quantum sensing, and evaluation of QIS (including QIS-secure) applications; a national computational infrastructure to support this initiative;

[90] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. SEC. 9414. *Study on Chinese Policies and Influence in the Development of International standards for Emerging Technologies* will produce an assessment of this issue for emerging technologies. SEC. 9414 is based on the "Ensuring American Leadership over International Standards Act of 2020," S. 4901, introduced on November 16, 2020, by Senator Cortez Masto (D-NV) and Senator Portman (R-OH), accessed March 26, 2021, https://www.congress.gov/bill/116th-congress/senate-bill/4901/text comprises.

[91] "Working Group 14 for Quantum computing was established by ITO/IEC JTC1 in June 2020," JTC1, accessed March 26, 2021, https://jtc1info.org/technology/working-groups/quantum-computing/. IEC and ISO have set up a working group (WG 14) in their joint technical committee on information technology (JTC1) to identify the standardization needs of quantum computing.

[92] "A 'China Model?' Beijing's Promotion of Alternative Global Norms and Standards," hearing before the U.S.-China Economic and Security Review Commission, 116th Congress, March 13, 2020, accessed March 26, 2021, https://www.uscc.gov/sites/default/files/2020-10/March_13_Hearing_and_April_27_Roundtable_Transcript.pdf.

[93] National Institute of Standards and Technology, "NIST's Post-Quantum Cryptography Program Enters 'Selection Round,'" July 22, 2020, accessed March 26, 2021, https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round.

[94] Dr. Carl J. Williams, "NIST's Program in Quantum Information Science," accessed April 16, 2016, https://science.osti.gov/-/media/nqiac/pdf/NIST_-presentation-NQIAC-20201027.pdf?la=en&hash=79A89EDF5BF6175360DF7EBCEB024F9B240B64A7.

engineering testbeds; programs to build a skilled QIS workforce; and participation by private industry (for example, the Quantum Economic Development Consortium[95]) to advance the development of a national QIS infrastructure and create fielded capabilities. In support of the National Quantum Coordinating Office, an interagency group led by the Department of Energy, NIST, and DARPA should oversee this infrastructure initiative, coordinating federal programs and guiding private industry's participation.

The administration should develop demonstration programs that show, in operational settings, national security implications of near-term quantum platforms. Some examples include the following:

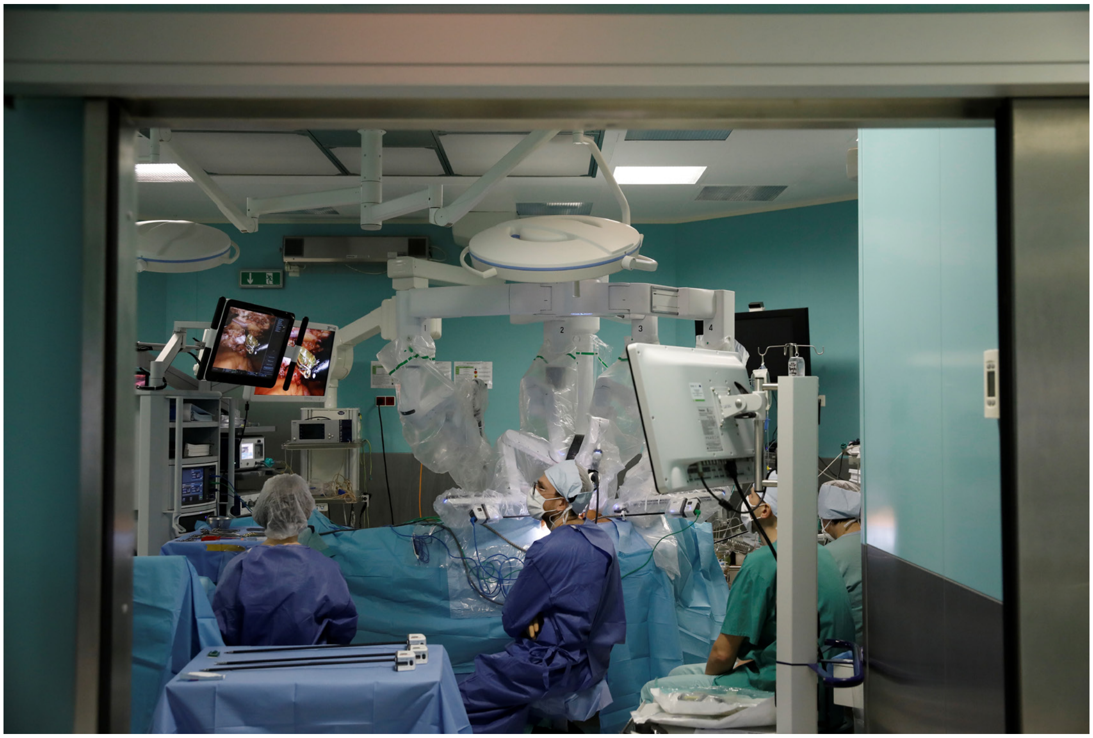
- **Quantum communications:** There are two areas of interest: (i) understanding vulnerabilities of various public key cryptographic systems to future quantum computing systems, an effort currently underway at NIST in the development of quantum resilient encryption standards, and (ii) use of QKD in large-scale demonstrations relevant to commercial and security applications, including space communications. QKD provides an approach to post-quantum communications security that is based on quantum phenomena, not algorithmic complexity.
- **Quantum computing:** Using small quantum computers in networked clusters or in hybrid architectures with classical computers.
- **Quantum networks:** The use of quantum networks for long-range quantum communications.
- **Quantum sensing:** Using quantum mechanics phenomena and devices for high-sensitivity and precision applications in sensing and communication, life sciences, and other fields.

The administration, through the National Quantum Coordinating Office, should establish funded competitions to improve the exchange of intellectual property and foster a common understanding across the government, industry, academic communities, and foreign institutions working on QIS.[96]

[95] National Institute of Standards and Technology, "NIST Launches Consortium to Support Development of Quantum Industry," September 28, 2018, accessed March 25, 2021, https://www.nist.gov/news-events/news/2018/09/nist-launches-consortium-support-development-quantum-industry. The Quantum Economic Development Consortium (QEDC) is a public-private partnership in the United States tasked with developing the future workforce needs for the QIS economy. Virtually all of the US private sector quantum companies are represented in the QEDC.

[96] J. Bienfang et al., *Building the Foundations for Quantum Industry*, NIST, June 20, 2018, accessed March 26, 2021, https://www.nist.gov/system/files/documents/2018/06/20/report-on-qid-v10.pdf.

Chapter 3. Enhanced Trust and Confidence in the Digital Economy



Surgical team is seen during a by-pass implantation operation using the Da Vinci robot at the MSWiA (Ministry of Interior and Administration) hospital in Warsaw Poland, March 16, 2021. Artificial intelligence in the healthcare sector may rapidly expand the capabilities of robot-assisted surgery and other critical processes. Picture taken March 16, 2021.

REUTERS/KACPER PEMPEL

Enhanced trust and confidence in the digital economy is founded upon personal privacy, data security, accountability for performance and adherence to standards, transparency of the internal decision-making algorithms, and regulations and governance for digital products and services. Trust and confidence in the digital economy is diminished by practices that do not protect privacy or secure data, and by a lack of legal and organizational governance to advance and enforce accountability.[97] Data breaches, malware embedded in downloaded apps, unfiltered mis- and disinformation, and the lack of governance models to effectively address these harms all contribute to the degradation of social and civic trust. This degradation

[97] Amon, "Toward a New Economy of Trust."

undermines economic and civic confidence, is costly,[98] constrains the growth of the digital economy,[99] and has destabilizing effects on society, governments, and markets. Trust and confidence in the digital economy is essential for open societies to function, and for resilience against cascading effects of local, regional, or national economic, security, or health instabilities.

Finding 3: To enhance trust and confidence in artificial intelligence and other digital capabilities, technologies must objectively meet the public's needs for privacy, security, transparency, and accountability.

The growth of digital economies is changing how trust is valued by institutions, businesses, and the public.[100] The traditional view of trust is expressed in terms of the security of a business transaction. The increase in cyberattacks, identity theft, social media disinformation campaigns, and the use of autonomous decision-making software, introduces new factors that affect trust. Trust in a firm's reputation and ethical practices, privacy protection, and how personal data are used depend on technology, business practices, and the public's perception of how well these components of trust are protected.

Not everyone has the same perception of what is trustworthy. However, reaping the benefits of the digital economy requires a high level of trust among users. Therefore, government and industry should work to enhance the transparency and accountability of digital systems to improve trustworthiness. Challenges include the following: (i) views on personal privacy protection are context-dependent, vary by culture or location, and may be formalized in different terms across nations, regions, and states; and (ii) as automated decision-making algorithms proliferate, new applications reveal trust weaknesses regarding implicit bias, unethical use of personal data, and lack of identity protection.

Trustworthiness needs to be prioritized and empirically demonstrated in the evolving market. Building trust involves educating all participants on the fundamental value of

[98] World Economic Forum, "Why trust in the digital economy is under threat," accessed March 26, 2021, http://reports.weforum.org/digital-transformation/building-trust-in-the-digital-economy/, citing an estimate by McAfee that the costs associated with cybersecurity incidents approximated $575 billion in 2014; Accenture, *Securing the Digital Economy: Reinventing the Internet for Trust*, 16, accessed March 26, 2021, https://www.accenture.com/us-en/insights/cybersecurity/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf#zoom=50. Cites five-year loss of foregone revenue from 2019 to 2023 to be $5.2 trillion, calculated using a sample of 4,700 global public companies.

[99] Congressional Research Service, *Digital Trade and U.S. Trade Policy*, 11, May 21, 2019, accessed March 26, 2021, https://crsreports.congress.gov/product/pdf/R/R44565; Alan B Davidson, "The Commerce Department's Digital Economy Agenda," Department of Commerce, November 9, 2015, accessed March 26, 2016, https://2014-2017.commerce.gov/news/blog/2015/11/commerce-departments-digital-economy-agenda.html Davidson identifies four pillars: promoting a free and open Internet worldwide; promoting trust online; ensuring access for workers, families, and companies; and promoting innovation.

[100] Frank Dickson, "The Five Elements of the Future of Trust," IDC, April 22, 2020, accessed March 26, 2021, https://blogs.idc.com/2020/04/22/the-five-elements-of-the-future-of-trust/.

trust in the digital economy and ensuring digital systems reflect individual and societal conceptions of trust. There must be national and international standards for judging how well technologies and systems protect trust. Professional organizations that audit for trust in the digital economy will strengthen accountability.

Finding 3.1: The European Union's General Data Protection Regulation uses data protection rules as a trust-enabler.[101]

As European Union (EU) member nations work to conform national rules and laws to the General Data Protection Regulation (GDPR), the European Commission notes that these steps may strengthen trust relationships. Other nations propose that a global framework for cross-border Internet policies may be able to protect data security and privacy while still allowing national laws and regulations as a part of the approach if certain trust relationships are maintained. For both approaches, a set of rules or principles provides the foundation for trust.

The GDPR[102] establishes regulations for data security and privacy that apply to any organization that collects or uses data related to people in the EU. The entire data chain is covered by the GDPR, including data collection, processing, storing, and managing.

The GDPR comprises principles that govern data protection and accountability for those who process data. There are technical measures for data security, and organizational design principles for data protection. Data privacy is expressed in terms of privacy rights, including the right: to be informed, to rectification, to erasure, to restrict processing, to data portability, and to object, and the right of access. There are also rights in relation to automated decision-making and profiling. The governance mechanism centers on Data Protection Authorities that work to align each EU member nation's approach to data security and privacy to conform with the GDPR. These Data Protection Authorities have enforcement powers and the ability to levy fines when a GDPR rule is violated.

Finding 3.2: Current approaches to machine learning and big data analytics risk weakening data protection rules.[103]

Data privacy protection is vulnerable to advanced data analytics that can infer personal identifiable information by joining loosely related data sources. As a result, the growing

[101] "Communication from the Commission to the European Parliament and the Council. Data protection rules as a trust-enabler in the EU and beyond – taking stock," COM/2019/374 final, European Union, July 24, 2019, accessed March 26, 2021, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2019:374:FIN.

[102] "General Data Protection Regulation," Intersoft Consulting, https://gdpr-info.eu/.

[103] T. Timan and Z.Á. Mann, eds., *Data protection in the era of artificial intelligence. Trends, existing solutions and recommendations for privacy-preserving technologies*, Big Data Value Association, October 2019, accessed March 26, 2021, https://www.bdva.eu/sites/default/files/Data%20protection%20in%20the%20era%20of%20big%20data%20for%20artificial%20intelligence_BDVA_FINAL.pdf.

use of current machine learning methods applied to large, multi-source data sets highlights potential limitations in the GDPR where such computational methods can infer data originally made private. The development of new data science capabilities may require research on new privacy-preserving technologies for nations to remain compliant with the GDPR. With increasing amounts of personal medical and genetic information being held in data repositories, this need is urgent.

Finding 3.3: Evolving US data privacy approaches consider outcome-based methods, versus prescriptive methods.

The development of data privacy laws in the United States is an evolving patchwork, with more than one hundred and fifty state data privacy laws proposed in 2019.[104] There is no overall federal data privacy law.

One instance of federal legislation for data privacy proposed in the 117th Congress[105] includes the following key privacy features, which are viewed as outcome-based.[106]

- Transparent communication of the privacy and data use policy
- Affirmative opt-in and opt-out consent
- Preemption, in which the proposed statute would preempt most state laws with limited exceptions for data breaches, and other limited situations
- A right to action, enforced at the federal or state level, to address alleged violations
- Independent audit of the effectiveness and appropriateness of the privacy policy for each entity providing data services

Several bills[107] introduced in the 116th Congress addressed a subset of the above features or are focused on COVID-19 contact tracing, health status, and identifiers. In addition,

[104] "2019 Consumer Data Privacy Legislation," National Conference of State Legislatures, January 3, 2020, accessed March 26, 2021, https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx.

[105] "Information Transparency and Personal Data Control Act," fact sheet, accessed March 26, 2021, https://delbene.house.gov/uploadedfiles/delbene_consumer_data_privacy_bill_fact_sheet.pdf; Information Transparency & Personal Data Control Act, H.R. 2013 — 116th Congress (2019-2020), accessed April 2, 2021, https://delbene.house.gov/uploadedfiles/delbene_privacy_bill_final.pdf.

[106] "Developing the Administration's Approach to Consumer Privacy," *Federal Register*, September 26, 2018, accessed March 26, 2021, https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrations-approach-to-consumer-privacy; Alan Charles Raul and Christopher Fonzone, "The Trump Administration's Approach to Data Privacy, and Next Steps," Sidley Austin LLP, October 2, 2018, accessed March 26, 2021, https://datamatters.sidley.com/the-trump-administrations-approach-to-data-privacy-and-next-steps.

[107] Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA Act), S.4626 — 116th Congress (2019-2020), https://www.congress.gov/116/bills/s4626/BILLS-116s4626is.pdf; Online Privacy Act of 2019 , H.R. 4978 — 116th Congress (2019-2020), https://www.congress.gov/bill/116th-congress/house-bill/4978/text; COVID-19 Consumer Data Protection Act of 2020, S. 3663 — 116th Congress (2019-2020), https://www.congress.gov/bill/116th-congress/senate-bill/3663.

several bills introduced in the 116th Congress addressed disclosing how data are used or monetized by social media companies that enhance the accessibility and portability of a user's data across devices.[108]

The National Institute of Standards and Technology (NIST) Privacy Framework describes a risk- and outcomes-based approach to establishing privacy protection practices in an organization. Organizations can vary the technologies and design of the privacy protection aimed at satisfying performance outcomes. This may be advantageous when the technologies and applications are changing at a fast pace, e.g., artificial intelligence (AI) and the Internet of Things (IoT).[109]

While there are several federal data privacy laws specific to certain industries or groups, e.g., the Health Insurance Portability and Accountability Act (HIPAA),[110] the eventual form and scope of US data protection laws will depend on policy and legal considerations. A key decision concerns the model for data protection laws. The EU GDPR model is prescriptive; GDPR compliance involves demonstrating that the procedural rules were followed. An alternate model for data protection laws is outcome-based, which allows flexibility in how to achieve data protection.[111]

A choice between prescriptive versus outcome-based approaches must assess their relative costs and benefits and how the two approaches can work together. The proposed bills in the 116th Congress identify a robust set of data privacy features while promoting flexibility and innovation in their implementation; the GDPR model has greater worldwide traction, creating opportunities for harmonized regulatory treatment.

Finding 3.4: New information technologies compel automated compliance testing.

New information technologies and advanced data capabilities challenge current methods of compliance and enforcement. The variety of new ways to collect, process, and analyze

[108] Designing Accounting Safeguards to Help Broaden Oversight and Regulations on Data Act, S. 1951 — 116th Congress (2019-2020), accessed March 26, 2021, https://www.congress.gov/bill/116th-congress/senate-bill/1951. The informal reference, DASHBOARD Act, is found in articles about this bill; Public Health Emergency Privacy Act, S. 3749 — 116th Congress (2019-2020), accessed March 26, 2021, https://www.congress.gov/bill/116th-congress/senate-bill/3749. This has been reintroduced in the 117th Congress. Mark R. Warner, Warner, Blumenthal, Eshoo, Schakowsky & DelBene Introduce the Public Health Emergency Privacy Act, press release, January 28, 2021, https://www.warner.senate.gov/public/index.cfm/2021/1/warner-blumenthal-eshoo-schakowsky-delbene-intro duce-the-public-health-emergency-privacy-act; Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act of 2019, S. 2658 — 116th Congress (2019-2020), accessed March 26, 2021, https://www.congress.gov/bill/116th-congress/senate-bill/2658.

[109] National Institute of Standards and Technology, "NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0," January 16 2020, accessed March 26, 2021, https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf.

[110] Congressional Research Service, *Data Protection Law: An Overview*, March 25, 2019, accessed March 26, 2021, https://fas.org/sgp/crs/misc/R45631.pdf.

[111] Ibid., 56.

data is increasing at a fast rate, while compliance often is determined on a case-by-case basis by regulatory and legal experts. To keep pace, automated testing for compliance with data privacy regulations is necessary.

Table 3 portrays some of the challenges and solutions for achieving automated compliance testing. This research agenda identifies the following key developments: standards, new privacy-preserving technologies, and automated methods to establish compliance.

Table 3. Big Data Value Association Strategic Research and Innovation Agenda

Challenges	Solutions
A general, easy-to-use, and enforceable data protection approach	Guidelines, standards, law, and codes of conduct
Maintaining robust data privacy with utility guarantees	Multiparty computation, federated learning approaches, and distributed ledger technologies
Risk-based approaches calibrating data controllers' obligations	Automated compliance, risk assessment tools
Combining different techniques for end-to-end data protection	Integration of approaches, toolboxes, overviews, and repositories of privacy-preserving technologies

SOURCE: TIMAN AND MANN 2019[112]

Privacy-preserving technologies are an active research area, and include the following:[113] secure multiparty computation, (fully) homomorphic encryption, trusted execution environments, differential privacy, and zero-knowledge proofs.

The value of privacy-preserving technologies involves trade-offs between privacy and utility—how useful is the resulting data—both of which are context dependent.[114] Affecting these trade-offs are the technical methods, the technical definitions of privacy, and the specifications of the privacy laws. The technical methods (e.g., anonymization, sanitization, and encryption) operate on data in different ways. The technical definition of privacy varies by application and the user's perceptions of risk versus the benefit of making personal data available. Privacy laws vary across nations, challenging the uniform application of technical methods. For both professionals and members of the public, making trade-offs between privacy and utility remains challenging. This is partially due to the absence of definitions of and standards for

[112] Timan and Mann, Data protection.

[113] Big Data UN Global Working Group, *UN Handbook on Privacy-Preserving Computation Techniques*, accessed March 26, 2021, https://marketplace.officialstatistics.org/privacy-preserving-techniques-handbook .

[114] Daniel Bachlechner, Karolina La Fors, and Alan M. Sears, "The Role of Privacy-Preserving Technologies in the Age of Big Data," proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy, San Francisco, December 13, 2018, accessed March 26, 2021, https://www.albany.edu/wisp/papers/WISP2018_paper_11.pdf; Felix T. Wu, "Defining Privacy and Utility in Data Sets," *University of Colorado Law Review* 84 (2013), accessed March 26, 2021, http://lawreview.colorado.edu/wp-content/uploads/2013/11/13.-Wu_710_s.pdf.

measuring privacy and the social benefits obtained from making data available for use by others.

Finding 3.5: Trust and confidence in digital capabilities requires businesses and governments to focus on the responsible use of technology.

Increasing trust and confidence in emerging technologies, such as AI, requires a recognition by both businesses and governments that they have an obligation to use technology responsibly, ensuring that technology has a positive impact on society, especially with regards to equality and inclusion.[115] Developing and innovating responsibly means ensuring that (i) ethical frameworks and policies exist to guide organizations during all aspects of a product's development and deployment, (ii) fairness in design is emphasized from the outset, and that (iii) questions around the manner in which technologies will be used are given the same rigorous examination as technical issues. As technological capabilities evolve and become more deeply intertwined in all aspects of society, businesses and governments must put ethics at the center of everything they do.

Approach 3: Build in trust-enabling technologies, measure performance against standards, conduct independent compliance audits.

The digital economy relies on achieving a high level of trust and confidence on a continuing basis as technologies evolve. Trust and confidence-enabling technologies must be developed and built into the components of the digital economy infrastructure; a detailed understanding of the trade-offs between privacy versus utility is an essential foundation. Such technologies must be paired with similar civic norms, practices, and rules designed to enhance confidence in the digital economy. To assure businesses that they remain compliant with data protection regulations as they modernize their practices, automated compliance testing, accompanied by standards of performance, is needed. To establish transparency for automated decision-making algorithms, standards for the measurable performance, i.e., the output results, are necessary. Independent assessments of the compliance testing and algorithmic transparency by professional auditing organizations could enhance trust among all participants in the digital economy and aid accountability and governance; such methods should be explored. However, mechanisms for compliance testing and auditing by regulators are also necessary.[116]

[115] Kirsten Martin, Katie Shilton, and Jeffrey Smith, "Business and the Ethical Implications of Technology: Introduction to the Symposium," *Journal of Business Ethics* 160, 307–317 (2019), accessed April 16, 2021, https://doi.org/10.1007/s10551-019-04213-9

[116] Nicholas Confessore, "Audit Approved of Facebook Policies, Even After Cambridge Analytica Leak," *New York Times*, April 19, 2018, accessed March 26, 2021, https://www.nytimes.com/2018/04/19/technology/facebook-audit-cambridge-analytica.html.

Recommendation 3: Develop international standards and best practices for a trusted digital economy that accommodate national rules and regulations, streamline the process of independently assessing adherence to these standards.

Recommendation 3.1: Develop a US data privacy standard.

Congress should create a national data privacy standard that embodies the following principles: (i) *appropriate use of data*: this defines the intended purpose for the collected data, the scope of what can be collected, the needed security, and the entities that are covered by the principle; (ii) *nondiscriminatory use*: the collected data cannot be used to discriminate against protected classes; (iii) *informed participation*: the individuals must receive the privacy policies in a transparent manner before data are collected, and provide affirmative express consent, including the ability to revoke consent and require destruction of the data or the movement of the data as directed by the individual (i.e., portability); (iv) *public reporting*: covered entities must periodically report on the data collected, retained, and destroyed, and the groups of individuals from whom the data were collected; (v) *independent audit*: the performance of covered entities with respect to the data privacy standard must be annually audited by an independent auditing organization, with parallel mechanisms to accommodate auditing and review by regulatory agencies; (vi) *enforcement*: federal and state enforcement organizations are given the authority to pursue violations of the laws for data privacy protection; (vii) *preemption*: this would preempt state privacy laws that are inconsistent with the proposed national standard; and (viii) *consumer protection laws*: the privacy standard would not interfere with consumer protection laws on issues apart from data privacy.

The data privacy standard should recognize gradations in the sensitivity of personal data—some personal data are treated more strictly than others. Affirmative express consent should be structured based on the types of data and how they will be used.

Congress should work to develop a national data privacy standard that can achieve global interoperability and should request an analysis of emerging privacy standards and issues that limit this achievement. Congress also should use the proposed national data privacy standard to inform the development of transparent national consumer data privacy laws that preserve individuals' control of their personal data and facilitate the development of trusted networks and applications.

The results should establish federal data privacy standards for personal data, establish standards for content moderation by information providers, and should regulate platform providers' ability to conduct experiments or surveys with users and user data without prior consent.

Recommendation 3.2: Develop privacy-preserving technologies for the digital economy and demonstrate in a full-scale test their conformance with the General Data Protection Regulation.

The administration should direct NIST to establish and test privacy-preserving technologies that enable a risk- and outcomes-based approach to trust in the digital economy. The test should evaluate, at scale, conformance with relevant GDPR rules, conformance with existing US laws governing data privacy, and robustness with respect to innovations and advances in information technologies and data capabilities, especially those based on AI, machine learning, and the IoT. This work should include the development of technical definitions of privacy and application-specific measures of the utility of analyses that are based on privacy-protected data. The tests should include end user evaluations.

The administration should establish a near-term program that demonstrates privacy-preserving technologies to aid the trusted collection and sharing of data for the purpose of improving individuals' access to healthcare during large-scale biological events. This program should be jointly managed by NIST, the Department of Health and Human Services (HHS), the National Institutes of Health (NIH), and the National Science Foundation (NSF). This program will monitor system performance to inform the development of standards for the ethical use of the shared data and how data governance will be formulated.

Recommendation 3.3: Create measurement methods and standards for evaluating trust in the digital economy.

The administration should direct the National Institute of Standards and Technology (NIST) to establish methods for evaluating users' trust in the digital economy given the increasing use of AI, big data analytics, and automated decision-making algorithms. This work builds on the Commission on Enhancing National Cybersecurity's *Report on Securing and Growing the Digital Economy*[117] and the *National Strategy for Trusted Identities in Cyberspace*.[118] One assessment framework example[119] describes measures of: "(i) user trust in the digital environment, e.g., data privacy, security, private sector efforts to control the spread of misinformation, and private sector adherence to cybersecurity best practices; (ii) the user experience, i.e., the effort needed to interact with

[117] Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy*, December 1, 2016, accessed March 26, 2021, https://www.nist.gov/system/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

[118] White House, "National Strategy for Trusted Identities in Cyberspace, Enhancing Online Choice, Efficiency, Security, and Privacy," April 2011, accessed March 26, 2021, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

[119] Bhaskar Chakravorti, Ajay Bhalla, and Ravi Shankar Chaturvedi, "How Digital Trust Varies Around the World," *Harvard Business Review*, February 25, 2021, accessed April 16, 2016, https://hbr.org/2021/02/how-digital-trust-varies-around-the-world.

the digital environment; (iii) user attitudes, e.g., how trusted are government and business leaders; and (iv) user behavior, i.e., how much do users interact with the digital environment."[120]

The administration should create a coalition to develop international standards for achieving trust in the digital economy. The coalition should include representatives from NIST, the Federal Trade Commission (FTC), private industry, Federally Funded Research and Development Centers (FFRDCs), University Affiliated Research Centers (UARCs), and international standards organizations. The United States and like-minded nations and partners should develop national assessments of trust in the digital economy using these standards.

Recommendation 3.4: Empower an organization to audit trust in the digital economy.

Congress should establish or empower an organization to audit the efficacy of measures designed to ensure trust in the digital economy and assess conformance to current and future standards designed to enhance and maintain such trust. Independent third parties or the Government Accountability Office (GAO) are examples of where such auditing organizations could be housed.

As part of this process, the auditing organization could provide recommendations to Congress on legislation that would enhance existing trust measures, develop new trust measures, and create trust performance standards. The auditing organization should also provide a mechanism through which the public and industry can raise topics and concerns for attention and, for cases where assessments or audits were done, include an ombudsman function for assessment appeals, identification of new information, or adjudication of concerns in a manner distinct from political influence.

The administration should work to establish a similar auditing program with EU members of the International Organization of Supreme Audit Institutions.

Recommendation 3.5: Assess standards relating to the trustworthiness of digital infrastructure.

Congress should direct an assessment by the National Academies of Sciences, Engineering, and Medicine of the current national and international standards relating to the trustworthiness of digital infrastructure to support the digital economy. "Trustworthiness of an information system is defined as the degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of

[120] Appendix A provides several references on the topics of trust and countering digital misinformation.

the information being processed, stored, or transmitted by the system across the full range of threats."[121]

Due to the increasing complexity of the digital infrastructure, the assessment should also review design standards for complex systems-of-systems from the perspective of trustworthiness. The overall assessment focuses on systems that support the digital economy. The study should assess the sufficiency of existing standards to guide improvements in trustworthiness, identify where new standards are needed, and recommend the data collection and testing methods that would enable ongoing assessments.

Recommendation 3.6: Educate the public on trustworthy digital information.

Congress should establish a grant program led by NSF for the purpose of developing a curriculum on trustworthiness of information—distinct from the trustworthiness of information systems—in the digital age. This curriculum should be created by a consortium headed by a university or coalition of universities. The program should be administered by select universities, with the participation of US information providers. The goal should be to educate the public on how to assess the trustworthiness of information—its credibility, truthfulness, and authenticity, and to develop tools that students and members of the public can use and benefit from on a regular basis.

[121] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5, September 2020, accessed April 16, 2021, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

Recommendation 3.7: Conduct demonstration projects involving artificial intelligence to improve delivery of public- and private-sector services at local, state, and federal levels.

Congress should authorize and appropriate funds for AI demonstration projects that improve the delivery of public services.[122] The overall program would be managed by one of the National Laboratories or by a newly created FFRDC with the mission to leverage technology to improve the delivery of public services. These testbed projects would be supported by local and state grants, cross-cutting federal government efforts, and public-private partnerships (PPPs) to employ AI to improve healthcare, workforce training, food production and distribution, and other areas. The overarching goals are to increase public trust in, understanding of, and confidence in AI; to learn how to use AI in ways that reduce inequality and enhance, rather than replace, human work; and to improve access, affordability, and availability of such services. At local, state, and federal levels, individual government agencies will gain long-term benefits by acquiring the necessary data infrastructure to employ AI to improve the delivery of public services.

Recommendation 3.8: Produce a framework for assessing ethical, social, trust, and governance considerations associated with specific current and future use cases for AI.

The administration should request the National Academy of Sciences to produce a framework for assessing ethical, social, trust, and governance considerations associated with specific current and future use cases for AI solutions. The framework should identify where new federal standards and rules are needed. This guidance should be developed with the participation of relevant executive branch departments and agencies, and in consultation with private industry, academia, members of the public, and government and industry representatives from foreign partners.

[122] A potential source for the types of initiatives of interest is the OECD Network of Experts on AI (ONE AI). This group provides policy, technical and business expert input to inform OECD analysis and recommendations. "OECD Network of Experts on AI (ONE AI)," OECD.AI, accessed March 26, 2021, https://www.oecd.ai/network-of-experts.

Chapter 4. Assured Supply Chains and System Resiliency

Sandia National Laboratories Engineer John Dillinger tests the security of a cargo container. Testing and evaluating new cargo security technologies has been a partnership between Sandia, the Space and Naval Warfare Systems Command (SPAWAR) Systems Center Pacific (SSC Pacific) and the Department of Homeland Security (DHS).

SCIENCE IN HD VIA UNSPLASH

Both physical and digital supply chain vulnerabilities can have cascading effects on the global economy and national security. Two critical examples include:

- **US dependence on foreign production of the main components used in generic drugs.** Trade disputes and economic crises can stop the flow of medicines and affect the health and economic welfare of tens of millions of individuals in the United States and other countries.[123]
- **US dependence on foreign-produced semiconductors for military and commercial products.** As the manufacturing and assembly of key components

[123] Congressional Research Service, *COVID-19: China Medical Supply Chains and Broader Trade Issues*, updated December 23, 2020, accessed March 26, 2021, https://crsreports.congress.gov/product/pdf/R/R46304.

shifts to markets in East Asia, particularly China,[124] the United States is susceptible to sudden interruptions in supplies and deliberate efforts to degrade the integrity of the products.

The interconnected global networks of manufacturing, transportation,[125] and distribution contain many instances where supply chain problems can have magnified effects. To protect against these diverse risks requires understanding which types of goods and sectors of the economy are critical. It also requires assessing the state and characteristics of supplies, trade networks and policies, inventory reserves, and the ability to substitute products or processing facilities. Assuring the performance of physical and software/IT supply chains is essential for a functioning, prosperous society and for national and economic security.

Finding 4: Resilient, trusted supply chains require defense, diversification, and reinvention.

One of the goals of the United States' National Strategy for Global Supply Chain Security[126] is to "foster a resilient supply chain." As part of its strategic approach, the national strategy works to prepare for, withstand, and recover from threats and disruptions. "Executive Order 13806 of July 21, 2017: Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States"[127] states that "a healthy manufacturing and defense industrial base and resilient supply chains are essential to the economic strength and national security of the United States" and requires a report detailing the current state of supply chains that are essential for national security. The Interagency Task Force report[128] in response to the executive order recommends decreasing the fragility and single points of failure of supply chains and diversifying away from dependencies on politically unstable countries.

It is difficult to know the full range of potential threats and disruptions for a given supply

[124] Department of Defense, *Fiscal Year 2020: Industrial Capabilities: Report to Congress*, January 2021, accessed March 26, 2021, https://media.defense.gov/2021/Jan/14/2002565311/-1/-1/0/FY20-INDUSTRIAL-CAPABILITIES-REPORT.PDF.

[125] Vivian Yee, "Ship Is Freed After a Costly Lesson in the Vulnerabilities of Sea Trade," *New York Times*, March 29, 2021, accessed April 3, 2021, https://www.nytimes.com/2021/03/29/world/middleeast/suez-canal-ever-given.html.

[126] "National Strategy for Global Supply Chain Security," Department of Homeland Security, last published July 13, 2017, accessed March 26, 2021, https://www.dhs.gov/national-strategy-global-supply-chain-security.

[127] "Executive Order 13806 of July 21, 2017: Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," *Federal Register* 82 (142) (July 26, 2017), accessed March 26, 2021, https://www.govinfo.gov/content/pkg/FR-2017-07-26/pdf/2017-15860.pdf.

[128] Department of Defense, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States, Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806*, September 2018, accessed March 26, 2021, https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF.

chain. For multitiered supply chains, the primary suppliers may not have information on each of the suppliers at the third or fourth tier and will not have accurate or up-to-date information on the trustworthiness of the sources of components, e.g., circuit board component suppliers. The multiplying, dynamic effects of supply chain disturbances are often not deterministic. In cases of deliberate sabotage of a resource, there may not be observable indicators, as with the insertion of hidden back doors in software. Resilient supply chains address a portion of these uncertainties through risk-reduction strategies and greater supply chain transparency.

For some supply chains, resilience may be attained by increasing defenses through greater trade enforcement and strengthening key segments. For some supply chains, diversifying the sources and manufacturing locations, in partnership with allies, is an effective strategy. Adversaries are creating strategic vulnerabilities and weaknesses in US supply chains; a key area is the design and manufacture of advanced electronics. To address this growing risk, the strategy exemplified in the Defense Advanced Research Projects Agency's (DARPA's) Electronics Resurgence Initiative[129] involves developing new technologies for alternative materials, designs, and production processes.

Finding 4.1: Critical supply chains are pervasive and challenging to defend.

Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience," defines critical infrastructure to be those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[130] There are eighteen critical infrastructure sectors. The Sector-Specific Plans discuss critical infrastructure resilience and include the supply chains in the risk management or risk mitigation section of some sector plans.

Supply chain attacks can be hard to detect and defend against. The Department of Defense's (DoD's) report, *Department of Defense Strategy for Operating in Cyberspace*,[131] highlights the critical issue of supply chain vulnerabilities and the risks of US reliance on foreign suppliers. The range of supply chain attack opportunities is large—including design, manufacturing, servicing, distribution, and disposal segments of the supply chain—and challenging to detect.

[129] "DARPA Electronics Resurgence Initiative," DARPA, last updated April 2, 2020, accessed March 26, 2021, https://www.darpa.mil/work-with-us/electronics-resurgence-initiative.

[130] White House, "Presidential Policy Directive – Critical Infrastructure Security and Resilience," February 12, 2013, accessed March 26, 2021, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[131] Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011, accessed March 26, 2021, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

Appendix B discusses the cyberattack of FireEye, involving the theft of its penetration testing toolkit, and the breadth of a comprehensive cyber espionage campaign centered on SolarWinds' Orion network monitoring software. More than eighteen thousand commercial and government targets, including Intel, Microsoft, California state hospitals,[132] the National Nuclear Security Administration,[133] and dozens[134] of federal, state, and local government agencies, downloaded compromised updates, all with the goal of extracting valuable intelligence while remaining undetected.

Finding 4.2: A broadened view of stockpiles increases resiliency.

Creating additional supplies or increasing production capacity contribute to creating stockpiles in a supply network. Adding more production capacity in the United States, or encouraging allies to undertake similar actions, is the focus of recent legislative efforts.

The Coronavirus Aid, Relief, and Economic Security Act (CARES Act; P.L. 116-136) strengthened reporting requirements to delineate the domestic versus foreign production of finished drug products and active pharmaceutical ingredients. While the CARES Act requires the National Academies of Sciences, Engineering, and Medicine to evaluate the US medical product supply chain, options for increasing the security and resilience of this supply chain are still under consideration.[135]

The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021[136] includes provisions to enhance the security of the semiconductor supply chain. It incentivizes investment in facilities and equipment in the United States for

[132] Laura Hautala, "SolarWinds hackers accessed DHS acting secretary's emails: What you need to know," c|net, March 29, 2021, accessed April 16, 2021, https://www.cnet.com/news/solarwinds-hackers-accessed-dhs-acting-secretarys-emails-what-you-need-to-know/

[133] Natasha Bertrand and Eric Wolff, "Nuclear weapons agency breached amid massive cyber onslaught," *Politico*, December 17, 2020, accessed March 26, 2021, https://www.*politico*.com/news/2020/12/17/nuclear-agency-hacked-officials-inform-congress-447855.

[134] Raphael Satter, "U.S. cyber agency says SolarWinds hackers are 'impacting' state, local governments," Reuters, December 23, 2020, accessed March 26, 2021, https://www.reuters.com/article/us-global-cyber-usa-idUSKBN28Y09L.

[135] Congressional Research Service, *FDA's Role in the Medical Product Supply Chain and Considerations During COVID-19*, September 1, 2020, accessed March 26, 2021, https://crsreports.congress.gov/product/pdf/R/R46507.

[136] Samuel K. Moore, "U.S. Takes Strategic Step to Onshore Electronics Manufacturing," IEEE Spectrum, January 6, 2021, "The semiconductor strategy and investment portion of the *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* began as separate bills in the House of Representatives and the Senate. In the Senate, it was called the American Foundries Act of 2020, and was introduced in July and called for $15 billion for state-of-the-art construction or modernization and $5 billion in R&D spending, including $2 billion for the Defense Advanced Research Projects Agency's Electronics Resurgence Initiative. In the House, the *Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America Act*, was introduced in the 116th Congress by Senators John Cornyn (R-TX) and Mark Warner (D-VA), and Representatives Michael McCaul (R-TX) and Doris Matsui (D-CA), and offered similar levels of R&D," accessed April 16, 2021, https://spectrum.ieee.org/tech-talk/semiconductors/processors/us-takes-strategic-step-to-onshore-electronics-manufacturing.

semiconductor fabrication, assembly, testing, advanced packaging, or R&D. It strengthens the United States' capacity to develop and produce cutting-edge semiconductors domestically through federal funding, promotes greater global transparency around subsidies to identify unfair or opaque forms of support that distort global supply chains, and provides funding support to "foreign government partners to participate in a consortium in order to promote consistency in policies related to microelectronics, greater transparency in microelectronic supply chains, and greater alignment in policies toward non-market economies."[137]

"Executive Order 13817 of December 20, 2017: A Federal Strategy to Ensure Secure and Reliable Supplies of Critical Minerals" defines "critical mineral" to be "(i) a non-fuel mineral or mineral material essential to the economic and national security of the United States, (ii) the supply chain of which is vulnerable to disruption, and (iii) that serves an essential function in the manufacturing of a product, the absence of which would have significant consequences for our economy or our national security."[138] Based on country production and import reliance, thirty-five minerals were deemed critical minerals.[139] For some of these critical minerals, increased domestic production is possible,[140] through the policies in the executive order intended to decrease the time to obtain mining permits.

The DoD is working to ensure reliable supplies of rare earth minerals by increasing domestic production and processing capabilities.[141] The department has taken steps to increase stockpiles, reduce reliance on Chinese sources, partner with private industry to increase production of rare earth magnets, and accelerate the development of new rare earth mineral processing technologies, and is seeking to increase funding for domestic production of rare earth minerals for munitions and missiles. To increase domestic production of rare earth minerals, mining-reform legislation is needed. The

[137] US Sen. Mark R. Warner (D-VA), Bipartisan, Bicameral Bill Will Help Bring Production of Semiconductors, Critical to National Security, Back to U.S., press release, June 10, 2020, accessed March 26, 2021, https://www.warner.senate.gov/public/index.cfm/2020/6/bipartisan-bicameral-bill-will-help-bring-production-of-semiconductors-critical-to-national-security-back-to-u-s.

[138] "Executive Order 13817 of December 20, 2017: A Federal Strategy To Ensure Secure and Reliable Supplies of Critical Minerals," *Federal Register*, December 20, 2017, accessed March 26, 2021, https://www.federalregister.gov/documents/2017/12/26/2017-27899/a-federal-strategy-to-ensure-secure-and-reliable-supplies-of-critical-minerals.

[139] Aluminum (bauxite), antimony, arsenic, barite, beryllium, bismuth, cesium, chromium, cobalt, fluorspar, gallium, germanium, graphite (natural), hafnium, helium, indium, lithium, magnesium, manganese, niobium, platinum group metals, potash, the rare earth elements group, rhenium, rubidium, scandium, strontium, tantalum, tellurium, tin, titanium, tungsten, uranium, vanadium, and zirconium.

[140] National Strategic and Critical Minerals Production Act, H.R. 2531 — 116th Congress (2019-2020), accessed March 26, 2021, https://www.congress.gov/bill/116th-congress/house-bill/2531. The bill aims to increase the domestic supply of critical minerals.

[141] Department of Defense, DOD Announces Rare Earth Element Awards to Strengthen Domestic Industrial Base, press release, November 17, 2020, accessed March 26, 2021, https://www.defense.gov/Newsroom/Releases/Release/Article/2418542/dod-announces-rare-earth-element-awards-to-strengthen-domestic-industrial-base/.

current mine-permitting process takes approximately ten years, when timelines of two to three years may be possible. Cooperative agreements with like-minded countries may also increase the supply available to the United States. South Africa, Canada, Australia, Brazil, India, Malaysia, and Malawi have rare earth minerals; China, Russia, and the United States hold 82.6 percent of the world's production and reserves.[142]

Finding 4.3: By creating new materials and new design and manufacturing technologies, the United States can eliminate critical dependencies on foreign sources.

The DARPA Electronics Resurgence Initiative[143] is in the fourth year of a long-term, $1.5 billion effort to reinvent defense electronics both to improve performance and to respond to foreign efforts to shift innovation in electronics away from the United States. The program currently includes applications of the new materials, chip designs, chip manufacturing technologies, and new methods for increasing security in a variety of defense systems. At present, the United States imports 80 percent of its rare earth elements directly from China.

The DARPA Electronics Resurgence Initiative supports the goals of the "Executive Order 13953 of September 30, 2020: Addressing the Threat to the Domestic Supply Chain From Reliance on Critical Minerals From Foreign Adversaries and Supporting the Domestic Mining and Processing Industries." The transformation of microelectronics is DoD's top modernization priority. A critical, fundamental risk is the US dependence on foreign semiconductor chip manufacturing, dominated by microelectronics fabrication plants in vulnerable Taiwan and South Korea.

Approach 4: Develop supply chain resilience strategies for a broadened set of critical resources, conduct assessments with allies.

The United States must establish criteria for determining which supply chains are critical and develop supply chain assurance strategies based on knowledge of the current supply network and the creation of alternative pathways, processes, and materials. Such strategies must incorporate (i) a supplier nation's trade and export policies and the effects of sudden changes, (ii) a nation's near-monopoly of a key resource, (iii) alternate supply lines available to the United States, (iv) baseline capacities and resources, and (v) the ability to reestablish commercial operations in locations having lower risk.[144]

[142] Marc Humphries, *Rare Earth Elements: The Global Supply Chain*, Congressional Research Service, December 16, 2013, accessed March 26, 2021, https://fas.org/sgp/crs/natsec/R41347.pdf.

[143] "DARPA Electronics Resurgence Initiative," DARPA.

[144] Congressional Research Service, *COVID-19: China Medical Supply Chains and Broader Trade Issues*, R46304, April 6, 2020, updated December 23, 2020, accessed March 26, 2021, https://crsreports.congress.gov/product/pdf/R/R46304.

For information systems and networks, the United States should develop and test cybersecurity resilience strategies and performance standards for increased cybersecurity in systems that support supply chains for critical resources.

Recommendation 4: Conduct regularized assessments in the United States and in allied countries to determine critical supply chain resilience and trust, implement risk-based assurance measures. Establish coordinated cybersecurity acquisition across government networks and create more experts.

Recommendation 4.1: Implement a framework that identifies and establishes global data collection on critical resources.

"Executive Order 14017 of February 24, 2021: America's Supply Chains," will conduct a review of critical supply chain vulnerabilities affecting both government procurement and also that of the private sector. This review will address the changing nature of critical supply chains as "manufacturing and other needed capacities of the United States modernize to meet future needs."[145] It will examine dependence on foreign suppliers, measures of resilience, and a range of sectors including energy, semiconductors, key electronics and related technologies, telecommunications infrastructure, and key raw materials. Strategies to increase critical supply chain resilience include "a combination of increased domestic production, strategic stockpiles sized to meet our needs, cracking down on anti-competitive practices that threaten supply chains, implementing smart plans to surge capacity in a time of crisis, and working closely with allies."[146] After this initial review, the administration plans to ask Congress to enact a mandatory quadrennial critical supply chain review to institute this process permanently.

To conduct this critical supply chain review, the administration should develop a set of criteria for determining resources that are critical to the nation with respect to public health, national security, economic security, and technological competitiveness. These criteria should encompass critical resources beyond high-technology products, to include IT and computer systems and infrastructures, and lower technology products that are important for high-technology competitiveness, e.g., steel, auto parts, and other portions of US manufacturing industries. These criteria should be developed by the White House Office of Science and Technology Policy (OSTP) in coordination with relevant executive branch agencies and departments and with

[145] "Executive Order on America's Supply Chains," White House, February 24, 2021, accessed March 26, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/; "Executive Order 14017 of February 24, 2021, America's Supply Chains," *Federal Register*, March 1, 2021, https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains.

[146] "The Biden Plan to Rebuild U.S. Supply Chains and Ensure the U.S. Does Not Face Future Shortages of Critical Equipment," accessed March 26, 2021, https://joebiden.com/supplychains/.

the active participation of private industry. Because critical resources are dynamic in nature and are constantly evolving, this should be a recurring, ongoing initiative.

The administration should use existing fora for international outreach to foster data collection and information sharing for assessments of critical resources and critical supply chains. It should also identify where US funding will strengthen supply chain assurance in partner countries, particularly those with a strong rule of law and a commitment to intellectual property protection. The assessments must address where key resources (e.g., pharmaceuticals,[147] agricultural products[148]) are manufactured and sourced, and how this impacts the robustness of US supply chains, the ability to manufacture the key resources in the United States, and other issues concerning supply chain threats and vulnerabilities. The United States-Mexico-Canada Agreement (USMCA) in its "Rules of Origin" chapter provides a model for agreements with like-minded countries.[149] The United States Trade Representative would develop trade agreements that help strengthen supply chains.

Recommendation 4.2: Fund and broaden federal oversight of supply chain assurance to include all critical resources.

Congress should establish an annual reporting requirement that assesses the supply chain assurance for all critical resources, to be assigned to the Department of Homeland Security (DHS) with support from the Office of Management and Budget (OMB). The Cybersecurity and Infrastructure Security Agency (CISA) will contribute assessments of the cybersecurity of the supply chains included in the annual report. This report should determine priorities for supply chains deemed critical to US national and economic security and national health. Congress should require that federal budget requests affecting critical supply chains are based on these priorities.

The administration should develop an approach to address risk management for supply chains beyond those already associated with information technology and computer systems. The administration should extend the work by NIST to model critical assets

[147] OECD and European Union Intellectual Property Office, *Trade in Counterfeit Pharmaceutical Products*, (Paris: OECD Publishing, 2020), accessed March 26, 2021, https://doi.org/10.1787/a7c7e054-en; Agnes Shanley, "Focusing on the Last Link," PharmaTech, September 2, 2018, accessed March 26, 2021, https://www.pharmtech.com/view/focusing-last-link; *Eurohealth*, Quarterly of the European Observatory on Health Systems and Policies 24 (3) (2018), accessed March 26, 2021, https://www.euro.who.int/__data/assets/pdf_file/0011/382682/*eurohealth*-vol24-no3-2018-eng.pdf?ua=1.

[148] Clara Frezal and Grégoire Garsous, "New digital technologies to tackle trade in illegal pesticides," OECD Trade and Environment Working Papers 2020/02, OECD Publishing, accessed March 26, 2021, https://doi.org/10.1787/9383b310-en.

[149] "Agreement between the United States of America, the United Mexican States, and Canada 7/1/20 Text," Office of the United States Trade Representative, accessed March 26, 2021, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between/.

and components for information systems,[150] to critical resources as described here. This effort will delineate the data—for both physical supply chains and software/IT supply chains—required to perform supply chain assurance assessments.

Recommendation 4.3: For the United States, the administration must develop a geopolitical deterrence strategy that addresses critical digital resources and digital supply chain assurance.

State-based cyber-enabled threats to the integrity of global supply chains—impacting both physical (as seen in disruption to global logistics and manufacturing activity in the wake of the NotPetya ransomware attack[151]) and digital (as illustrated in the wake of the SolarWinds compromise) supply chains—increasingly represent costly and high-impact challenges. The national cyber director, as part of the National Cyber Strategy, should develop a geopolitical deterrence strategy that enables the US government to leverage all tools of US power—from diplomacy, to sanctions, cyber, and military activity—to exercise deterrence. The administration should evaluate the potential for (i) continuous evaluation of digital supply chains to enable prompt detection of malicious activity targeting these supply chains, and (ii) prompt detection, combined with improved supply chain resilience and timely actions in response to the detected activity, to decrease the likelihood of cyberattacks. Continuous evaluation of supply chains for critical digital resources[152] would be coordinated and managed by CISA as part of its role in managing federal cybersecurity risk.

Recommendation 4.4: Conduct regular physical and software/IT supply chain assessments in the United States and with allies, focused on intersecting vulnerabilities with cascading consequences.

The administration should establish with allies and partner nations a test program for supply chains and reporting on supply chains' status and test results. This reporting would address the readiness status of both public and private sector supply chains, and the results of exercises that test the preparedness, adequacy, and resiliency of supply chains against a range of conditions and scenarios, much like stress tests for the financial sector.

- Because most of the supply chain data are held by private companies, a key issue is whether the private sector will provide enough data about its supply

[150] "NISTIR 8179, Criticality Analysis Process Model: Helping Organizations Decide Which Assets Need to Be Secured First," National Institute of Standards and Technology, April 11, 2018, accessed March 26, 2021, https://csrc.nist.gov/News/2018/NISTIR-8179-Criticality-Analysis-Process-Model.

[151] Andy Greenberg, "The Untold Story of NotPetya, the most Devasting Cyberattack in History," *Wired*, August 22, 2018, accessed March 26, 2021, https://www.*wired*.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[152] A key enabler of continuous evaluation comprises software configuration databases which will permit visibility and traceability of software/IT supply chains. These require development.

> chains, or can be incentivized to do so. Questions to address include: what is the minimal information that is needed to calculate these performance measures, and will the resultant tests provide useful results across the situations of interest? will the private sector give these data, given its competitive positions? what is the best estimate of the metrics subject to the data availability constraints? Thus, the tests must show these estimates can be developed using acceptable access to the private data, or must determine a narrower set of criteria to test against.

Due to the many factors bearing on cybersecurity resilience, including the growing threat of sophisticated cyberattacks by major adversaries, the administration should develop software/IT supply chain resilience risk assessments that incorporate the effects of new standards and tools to measure cyber vulnerabilities, improved information sharing (including intelligence information on nation state-supported cyberattacks and ransomware denial of service attacks), designs for improvements that protect against systemic vulnerabilities, and new technologies such as cloud-based services.

Chapter 5. Continuous Global Health Protection and Global Wellness

People receive their coronavirus disease (COVID-19) vaccines at a mass vaccination site at Lumen Field Event Center in Seattle, Washington, U.S. March 13, 2021.

REUTERS/LINDSEY WASSON TPX IMAGES OF THE DAY

The COVID-19 pandemic has disrupted health and economic security, both directly and indirectly, for most of the planet. Inherent to this disruption are three systemic problems: (i) global and national leaders acted slowly to detect and contain the spread of the virus, (ii) global health organizations reacted slowly to contain the spread of the virus, and (iii) a mixture of factors caused the delayed response including late recognition of the threat and where it was circulating, slow incorporation of science and data into decision making, poor political will, and inconsistent messaging to citizens regarding the nature of the threat and precautions to take. The origin and spread of the coronavirus that causes COVID-19 also depended on a number of codependent factors—human encroachment on animal habitats, globalization and an interconnected world, and a global economy that ignored insufficient sanitation and public health standards. But, most importantly, it depended on a failure of adequate monitoring, data sharing, and early warning and mitigation systems.

Viruses and other pathogens know no borders, nor do they discriminate by race or class. Though nations may adopt their own strategies to enhance resilience and future planning, a more global approach to this interconnected system will be essential to keep all humans safe. Continuous global health protection builds upon a foundation of secure data and communications, rapid sharing of biological threat data across the globe, enhanced trust and confidence in the digital economy, and assured supply chains.

Finding 5: There is a need for a continuous biological surveillance, detection, and prevention capability.

The design of a pandemic surveillance, detection, and prevention system would require a multipronged approach, comprising global monitoring, early detection, rapid warning, and capable mitigation and prevention strategies. The system would perform the following main functions: biothreat agent recognition, mobilization of defenses, containing the spread of the biothreat agent, administration of therapeutic treatment, and the ability to recognize new pathogens and form specific neutralizing responses.

Much of the integrative assessments performed by the system would need to rely on a network capable of receiving data from multiple, decentralized information sources, and converting that information into indicators that can be aggregated and evaluated to support decision making at the individual, local community, and population level.[153] A global detection and response system could enable greater resilience and prevention, and decrease the potential that new outbreaks of pathogens lead to global pandemics.[154]

Finding 5.1: An early detection and warning system[155] requires global data collection of pathogen-related indicators, sometimes requiring novel sources to address information gaps.

Early detection would require the funding of a global, interconnected system that relies on partnerships among national governments and regional partners. Where there are gaps in collecting and sharing preferred data, e.g., when a nation or region

[153] National Syndromic Surveillance Program, “North Carolina Integrates Data from Disaster Medical Assistance Teams for Improved Situational Awareness,” Centers for Disease Control and Prevention, accessed March 26, 2021, https://www.cdc.gov/nssp/success-stories/NC-Disaster-Teams.html; “Influenza - Surveillance and monitoring,” World Health Organization, accessed March 26, 2021, https://www.who.int/influenza/surveillance_monitoring/en/.

[154] “World Health Organization, Global Influenza Surveillance and Response System,” World Health Organization, accessed March 26, 2021, https://www.who.int/influenza/gisrs_laboratory/updates/GISRS_one_pager_2018_EN.pdf?ua=1.

[155] “Toward the Development of Disease Early Warning Systems,” in *Under the Weather: Climate, Ecosystems, and Infectious Disease*, National Research Council (US) Committee on Climate, Ecosystems, Infectious Diseases, and Human Health [Washington, DC: National Academies Press (US), 2001], https://www.ncbi.nlm.nih.gov/books/NBK222241/.

does not participate, alternative indicators would need to be developed.[156]

The development of novel, authenticated data sources is a key risk factor for pandemic warning systems. As seen at the start of the COVID-19 pandemic, relying on government-provided information led to a delay in identifying the unusual pneumonia-like illness in Wuhan, China, and ultimately in releasing the genetic sequence of the virus.[157] It cost lives, delayed warnings and the ability for others to detect the circulating virus, delayed containment and mitigation strategies (e.g., vaccine and therapeutic development), and enabled the virus to spread globally via human vectors.[158]

Authenticated data sources from different decentralized sources and edge devices could include both traditional (e.g., positive viral tests, hospitalization rates, excess death rates) and nontraditional sources of health information (e.g., passive monitoring of environment, wastewater, satellite data, human migration trends, market signals) that can be overlaid, combined, and aggregated to understand current public health conditions and to have predictive value.

Finding 5.2: An elevated capacity on the global stage is required.

The components of global capacity in a pandemic include the ability to quickly identify and sequence novel pathogens; to quickly share that information with the world; to rapidly ramp-up testing; to develop and approve targeted vaccines and therapeutics; to have medical supply chain, manufacturing, and distribution capabilities in place; to have sufficient capital health equipment, medical consumables, and healthcare personnel in place; and to provide access to healthcare and reliable health information to all those in need.

[156] Sylvia Mathews Burwell et al., “Improving Pandemic Preparedness: Lessons From COVID-19,” Independent Task Force Report No. 78, Council on Foreign Relations, October 2020, accessed March 26, 2021, https://www.cfr.org/report/pandemic-preparedness-lessons-COVID-19/pdf/TFR_Pandemic_Preparedness.pdf; Elias Kondilis et al., “COVID-19 data gaps and lack of transparency undermine pandemic response,” *Journal of Public Health*, February 9, 2021, fdab016, https://doi.org/10.1093/pubmed/fdab016; Kamran Ahmed et al., “Novel Approach to Support Rapid Data Collection, Management, and Visualization During the COVID-19 Outbreak Response in the World Health Organization African Region: Development of a Data Summarization and Visualization Tool,” *JMIR Public Health and Surveillance* 6 (4) (Oct-Dec, 2020), accessed March 26, 2021, https://publichealth.jmir.org/2020/4/e20355/; Sameer Saran et al., “Review of Geospatial Technology for Infectious Disease Surveillance: Use Case on COVID-19,” *Journal of the Indian Society of Remote Sensing* 48 (2020): 1121–1138, accessed March 26, 2021, https://doi.org/10.1007/s12524-020-01140-5.

[157] Associated Press, “China didn’t warn public of likely pandemic for 6 key days,” April 15, 2020, accessed March 26, 2021, https://apnews.com/68a9e1b91de4ffc166acd6012d82c2f9.

[158] Jin Wu et al., “How the Virus Got Out,” *New York Times*, March 22, 2020, accessed March 26, 2021, https://www.nytimes.com/interactive/2020/03/22/world/coronavirus-spread.html; Zhidong Cao et al., “Incorporating Human Movement Data to Improve Epidemiological Estimates for 2019-nCoV,” medRxiv, https://doi.org/10.1101/2020.02.07.20021071

These specific functions for creating a comprehensive global alert and response system and coordinating actions, as well as supporting localized capacity strengthening,[159] were made part of the World Health Organization's (WHO's) updated 2005 International Health Regulations (IHR)[160] and its pandemic preparedness plan.[161] "To help countries review and, if necessary, strengthen their ability to detect, assess, and respond to public health events, WHO develops guidelines, technical materials, and training and fosters networks for sharing expertise and best practices. WHO's help supports countries in meeting their commitments under the IHR to build capacity for all kinds of public health events."[162]

To achieve the fullest potential of these approaches, there need to be investments on a global scale to support expanded detection, mitigation, and capacity-building strategies. These efforts should be conducted through public, private, and government partnerships based on mutual agreements to share data and report issues early. These should be multinational collaborations that would be able to overcome the limiting factors discussed in the next section. In developing these approaches, a priority is to strengthen transparency and accountability within the United Nations (UN) system, including at the WHO.[163]

Finding 5.3: There are several limiting factors.

There often is a lack of trust among groups, institutions, and governments. Governments do not always trust other governments; countries do not always trust global health bodies; nationally, states do not always trust each other or the federal government; and individuals do not always trust governments or health entities or officials. This lack of trust is well-documented. According to the 2020 Edelman Trust

[159] "Strengthening health security by implementing the International Health Regulations (2005), Country capacity strengthening," UN World Health Organization, accessed March 26, 2021, https://www.who.int/ihr/capacity-strengthening/en/.

[160] "Strengthening health security by implementing the International Health Regulations (2005), A global system for alert and response," World Health Organization, https://www.who.int/ihr/alert_and_response/en/; Apoorva Mandavilli, "239 Experts With One Big Claim: the Coronavirus Is Airborne," *New York Times*, updated November 19, 2020, accessed March 26, 2021, https://www.nytimes.com/2020/07/04/health/239-experts-with-one-big-claim-the-coronavirus-is-airborne.html.

[161] World Health Organization, *WHO global influenza preparedness plan: The role of WHO and recommendations for national measures before and during pandemics*, 2005, accessed March 26, 2021, https://www.who.int/csr/resources/publications/influenza/WHO_CDS_CSR_GIP_2005_5.pdf.

[162] "Strengthening health security by implementing the International Health Regulations (2005), Country capacity strengthening," UN World Health Organization, accessed March 26, 2021, https://www.who.int/ihr/capacity-strengthening/en/.

[163] Chairman Michael McCaul, *China Task Force Report*, U.S. House of Representatives, 116th Congress, September 2020, accessed March 26, 2021, https://gop-foreignaffairs.house.gov/wp-content/uploads/2020/09/CHINA-TASK-FORCE-REPORT-FINAL-9.30.20.pdf.

Barometer,[164] "no institution is seen as both competent and ethical," an opinion that includes government, business, nongovernmental organizations (NGOs), and the media. In the statistical model Edelman provides, government is widely seen as the most unethical, and the least competent, institution of the four. According to the International Development Association of the World Bank Group, half of the global population does not trust government institutions.[165] Similarly, both individual citizens and countries may lack trust in national and global health bodies.

Health institutions are concerned about sharing data on health outbreaks too early, as this could make them look underinformed, or to be "crying wolf" before the true measure of an outbreak is known.[166] Governments may be incentivized to withhold information on outbreaks to maintain appearances of strength and ultimately to control medical supplies to keep their own people safe. Withholding immediate access to information can severely affect outcomes, such as the spread of the virus, allowing it to gain a foothold in other countries unaware. It also prevents the type of global and interdisciplinary cross-collaboration that has been so effective at advancing science, research and development (R&D), and progress toward solutions.

The cost of developing and operating a global pandemic surveillance, detection, and warning and response system must be borne by all nations in an equitable manner. A recent study[167] estimates "[t]his cost includes the cumulative cost of failed vaccine candidates through the research and development process. … [P]rogressing at least one vaccine through to the end of phase 2a for each of the 11 epidemic infectious diseases would cost a minimum of $2.8–3.7 billion ($1.2 billion–$8.4 billion range)." According to a 2002 study, the cost of developing a vaccine—from research and discovery to product registration—is estimated to be between $200 million and $500 million per vaccine.[168] Due to the high costs of developing vaccines and current therapeutics, developing an equitable funding model will rely on new research to make vaccines less expensive to develop, new technologies to conduct wide-area detection of signatures of biological activity, and new techniques for inexpensive diagnostic testing worldwide. The supply

[164] "2020 Edelman Trust Barometer," Edelman, accessed March 26, 2021, https://www.edelman.com/trust/2020-trust-barometer.

[165] "Governance and Institutions," International Development Association, World Bank Group, accessed March 26, 2021, https://ida.worldbank.org/theme/governance-and-institutions.

[166] Stephen Buranyi, "The WHO v coronavirus: why it can't handle the pandemic," *Guardian*, April 10, 2020, accessed March 26, 2021, https://www.theguardian.com/news/2020/apr/10/world-health-organization-who-v-coronavirus-why-it-cant-handle-pandemic.

[167] Dimitrios Gouglas et al., "Estimating the cost of vaccine development against epidemic infectious diseases: a cost minimisation study," *Lancet Global Health* 6 (12) (E1386-E1396, DECEMBER 01, 2018), October 17, 2018, DOI: https://www.thelancet.com/journals/langlo/article/PIIS2214-109X(18)30346-2/fulltext, accessed March 26, 2021.

[168] Irina Serdobova and Marie-Paule Kieny, "Assembling a Global Vaccine Development Pipeline for Infectious Diseases in the Developing World," American *Journal of Public Health* 96 (9): 1554–1559, https://doi.org/10.2105/AJPH.2005.074583, accessed March 26, 2021.

chains, manufacturing capabilities, vaccines, and therapeutics must be developed in such a manner that all nations are protected by such a global pandemic prevention system. The concern extends beyond vaccines which have been developed. Some diseases, like Zika, for which no vaccines exist, continue to be studied; and parasites, such as those that cause malaria, may become more widespread due to global climate change.

There are many types and sources of data that need to be identified in order to effectively predict or fight an epidemic. One is vector tracking. It is difficult to track zoonotic vectors that lead to viral spread. It is estimated that wild animals, in particular mammals, harbor an estimated forty thousand unknown viruses, a quarter of which could potentially jump to humans;[169] it is also estimated that 75 percent of all emerging pathogens in the last decade have come from a zoonotic event.[170] Further, it is complicated to surveil and track pathogen genesis, evolution, and global spread. Understanding of the science of viruses, other pathogens, and their mutation and evolution is incomplete, and research continues on new ways to monitor and spot outbreaks.

Insufficient public health infrastructures. A 2017 study conducted by the World Bank and the WHO points out that half of the global population does not have access[171] to necessary health services, and one hundred million people live in extreme poverty.[172]

Approach 5: Develop a global pandemic surveillance, detection, and response system based on data sensing and integration via trusted networks.

Three important elements of this global system are the early detection and warning system, the rapid response and recovery system, and the elevated capacity building system.

[169] C.J. Carlson et al., "Global estimates of mammalian viral diversity accounting for host sharing," Nature Ecology & Evolution 3 (2019): 1070–1075 (2019), https://doi.org/10.1038/s41559-019-0910-6, accessed March 26, 2021. Global Virome Project / PREDICT has estimated that there are over 1.6 million unknown viral species in mammalian and avian populations, of which approximately 700,000 have the potential to infect and cause disease in humans. "Global Virome Project," https://static1.squarespace.com/static/581a4a856b8f5bc98311fb03/t/5ada612470a6ad672eea01b3/1524261157638/GVP%2B2%2Bpager%2BFINAL.pdf.

[170] Alex Long, "Zoonotic Diseases and the Possibilities with EBV Monitoring," *CTRL Forward*, November 14, 2017, accessed March 26, 2021, https://www.wilsoncenter.org/blog-post/zoonotic-diseases-and-the-possibilities-ebv-monitoring.

[171] World Health Organization, "World Bank and WHO: Half the world lacks access to essential health services, 100 million still pushed into extreme poverty because of health expenses," December 13, 2017, accessed March 26, 2021, https://www.who.int/news-room/detail/13-12-2017-world-bank-and-who-half-the-world-lacks-access-to-essential-health-services-100-million-still-pushed-into-extreme-poverty-because-of-health-expenses.

[172] "Health Financing: Key policy messages," World Health Organization, accessed March 26, 2021, https://www.who.int/health_financing/topics/financial-protection/key-policy-messages/en/.

Recommendation 5: Field and test new approaches that enable the world to accelerate the detection of biothreat agents, to universalize treatment methods, and to engage in mass remediation through multiple global means.

Recommendation 5.1: Develop a global early warning system comprised of pandemic surveillance systems coupled with an early warning strategy.

Congress should request the Centers for Disease Control and Prevention (CDC), National Institutes of Health (NIH), United States Agency for International Development (USAID), United States Department of Agriculture (USDA), and other associated agencies to jointly develop an initial demonstration of this system in collaboration with the WHO, private institutions, and partner nations. The foundation is a surveillance system comprised of both active and passive monitoring of multiple environments and biomes—space, atmosphere, water, soil, animal reservoirs. Fundamental to the pandemic surveillance strategy is (i) training locals to conduct routine testing and genomic surveillance where spillovers occur and to regularly report incidences of novel illnesses, and (ii) increased genetic testing to track pathogens and to delineate what is coming from the natural environment versus being weaponized. Funding contributions and expert participation from other nations should be obtained.

Early detection would be enhanced by increasing the ability to identify and aggregate known data signals, identifying novel data signals, and enabling the combination of these signals into meaningful public health insights. This requires data to be labeled in such a way that it is globally recognized, named, and usable. Detection and monitoring also depend on developing distributed networks upon which those secured signals can arrive, inform local testing and response activities, and eventually be aggregated, while protecting personal data privacy, so that insights can be extracted. Finally, after preliminary flags or warning indicators are observed, a threshold is crossed and the warning or alarm could be sent throughout the distributed network, rather than relying upon a single entity or body to release the relevant information.

Key development principles include: (i) first determine a sufficient and obtainable set of data that the surveillance system should collect, and develop the local and regional capabilities to collect these data; (ii) support a global, decentralized network that can authenticate data sources, and enable validated data-sharing amongst validated data producers; (iii) enable cybersecure data aggregation and analysis capabilities while preserving personal data based on the terms specified in Recommendation 3.1 in this report; (iv) empower a surveillance strategy commensurate with civil liberties and privacy protections; (v) facilitate a surveillance strategy comprised of both active and passive monitoring of multiple environments and biomes (space, atmosphere, water, soil); (vi) facilitate a surveillance strategy comprised of monitoring of traditional health and nontraditional data sources [e.g., excess death rates, viral genome sequences, Internet searches, geographic information systems (GIS), market trends]; and (vii) form distributed networks for global early warning system alerts.

Recommendation 5.2: Reestablish and realign existing pandemic monitoring programs.

The administration should provide R&D funding to current pandemic monitoring and response networks as part of the effort to build a system for continuous global health protection. The primary actions to consider include: reinstate the USAID PREDICT program[173] for tracking global zoonotic disease, provide additional funding to the Eco-Health Alliance,[174] and utilize networks to combine data being accumulated through parallel observation networks—e.g., the Strategic Advisory Group of Experts on Immunization (SAGE),[175] the National Ecological Observatory Network (NEON),[176] Collective and Augmented Intelligence Against COVID-19 (CAIAC),[177] and the Epidemic Intelligence from Open Sources (EIOS).[178]

Recommendation 5.3: Emphasize privacy protections in pandemic surveillance systems.

The administration should support initiatives that emphasize privacy protections in pandemic surveillance systems. These initiatives should be managed by NIST and NSF in collaboration with the Department of Health and Human Service's Office of the National Coordinator for Health Information Technology and the lead science institutions in partner nations. The mitigation strategies will (i) identify infected individuals early through robust and frequent testing with a globally-recommended strategy; (ii) deploy contact-tracing strategies (commensurate with civil liberties); (iii) deliver consistent health messaging for disease prevention, spread, and treatment by coordinating centralized information and data reporting with local, on-the-ground, trusted community leaders; and (iv) provide consistent public health guidance for gatherings like air travel, cruises, sporting events, schools, restaurants, stores, and so forth.

[173] PREDICT, "Reducing Pandemic Risk, Promoting Global Health," USAID, https://www.usaid.gov/sites/default/files/documents/1864/predict-global-flyer-508.pdf.

[174] "EcoHealth Alliance," website homepage accessed April 16, 2021, https://www.who.int/groups/strategic-advisory-group-of-experts-on-immunization/working-groups/cholera-(november-2015---august-2017).

[175] "Strategic Advisory Group of Experts on Immunization (SAGE)," World Health Organization, accessed April 16, 2021, https://www.who.int/groups/strategic-advisory-group-of-experts-on-immunization/working-groups/cholera-(november-2015---august-2017).

[176] "The National Science Foundation's National Ecological Observatory Network (NEON)," website homepage accessed April 16, 2021, https://www.neonscience.org/.

[177] "CAIAC: Collective and Augmented Intelligence Against COVID-19," website homepage accessed April 16, 2021, https://www.caiac19.org/.

[178] "Epidemic Intelligence from Open Sources (EIOS): Saving Lives through Early Detection," World Health Organization, https://www.who.int/initiatives/eios.

Recommendation 5.4: Increase resilience in medical supply chains.

The administration should fund R&D of cellular- and molecular-based manufacturing technologies[179] that enhance supply chain assurance.[180] Both cellular and molecular manufacturing are specific instances of synthetic biology. In some cases, they can be rapidly deployed by setting up the conditions for production, and then substituting in the genetic sequences of interest to go into high-gear production. This simplifies supply chain and production lead time, can increase capacity, and creates flexible supply chains by producing candidates that are thermostable.

Some of the more forward-looking technologies for bio-sensing, vaccine development, and therapeutics are amenable to this kind of manufacturing and stockpiling. The goal is to develop redundancy at a regional level (components/ingredients; manufacturing), adopt more rigorous methods for validation of authenticity, and support multiregional distribution chains.

Recommendation 5.5: Develop capacity building for vaccine and therapeutics discovery, development, and distribution.

The administration should establish PPPs to improve pandemic protection capacity building. There are three efforts: (i) biomanufacturing and synthetic biology innovations will create therapeutic discovery systems and speed vaccine discovery; (ii) vaccine discovery, development, and distribution coalitions like the Coalition for Epidemic Preparedness Innovations (CEPI) will enable equitable distribution; and (iii) information monitoring and distribution regarding consumables, capital equipment supplies, hospital resources, and healthcare workers will support public and organizational activities during a crisis.

Recommendation 5.6: Develop rapid responses to unknown pathogens, and supporting data collection networks.

NIH should develop and lead a program for the automated development of treatments for unknown pathogens. The goal is to universalize treatment methods; for example, by employing automated methods to massively select bacteriophages as a countermeasure to bacteria—or employ antibody-producing *E. coli* or cell-free synthetic biology as a countermeasure to viruses. Advanced computational methods such as computational

[179] Megan Scudellari, “Step Aside, PCR: CRISPR-based COVID-19 Tests Are Coming,” IEEE Spectrum, December 21, 2020, accessed April 16, 2021, https://spectrum.ieee.org/the-human-os/biomedical/diagnostics/step-aside-pcr-crispr-based-covid-19-tests-are-coming.

[180] Nicholas A. C. Jackson et al., “The promise of mRNA vaccines: a biotech and industrial perspective,” *npj Vaccines* 5 (11) (2020), https://doi.org/10.1038/s41541-020-0159-8, accessed March 26, 2021; Giulietta Maruggi et al., “mRNA as a Transformative Technology for Vaccine Development to Control Infectious Diseases,” *Molecular Therapy* 27 (4) (April 10, 2019): 757–772, accessed March 26, 2021, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6453507/.

modeling of the 3D molecules of novel pathogens, and AI-based selection of potential treatments, can help automate and speed up this process. New technologies that can change the time for the regulatory approval process, i.e., the time required for human clinical trials, should be researched—for example, in silico testing or artificial organ testing.[181]

NIH should create a consortium of universities and biotechnology companies to develop rapid, wide-area distribution of vaccines. This program should consider approaches that distribute vaccines through conventional supply channels, and methods to make vaccines that are survivable and transportable in any environment. Treatments in addition to vaccines should be incorporated in this effort.

NSF should create a digital infrastructure that can connect diverse, independent observation networks, databases, and computers—including emerging biosensors and autonomous sequencers deployed in water systems, air filtration systems, and other public infrastructure—to integrate their diverse data for analysis and modeling with protocols for activating rapid analysis of new pathogens, including new strains of extant pathogens to evaluate ongoing vaccine efficacy.

[181] Committee on Animal Models for Assessing Countermeasures to Bioterrorism Agents, Institute for Laboratory Animal Research Division on Earth and Life Studies, “Chapter 5: Alternative Approaches to Animal Testing for Biodefense Countermeasures,” in *Animal Models for Assessing Countermeasures to Bioterrorism Agents* (Washington, DC: The National Academies Press, 2011), accessed March 26, 2021, https://www.nap.edu/read/13233/chapter/7.

Chapter 6. Assured Space Operations for Public Benefit

Astronaut Franklin R. Chang-Diaz works with a grapple fixture during extravehicular activity to perform work on the International Space Station

NASA VIA UNSPLASH

The growing commercial space industry enables ready access to advanced space capabilities for a broader group of actors. To maintain trusted, secure, and technically superior space operations, the United States must ensure it is a leading provider of needed space services and innovation in launch, on-board servicing, remote sensing, communications, and ground infrastructures. A robust commercial space industry not only enhances the resilience of the US national security space system by increasing space industrial base capacity, workforce, and responsiveness, but also further advances a dynamic innovative environment that can bolster US competitiveness across existing industries, while facilitating the development of new ones.

As smaller satellites become more capable, large constellations of government and commercial platforms could increase space mission assurance and deterrence by "eliminating mission critical, single-node vulnerabilities and distributing space operations across hosts, orbits, spectrum, and geography."[182] Advances in commercial space also enable exploring our planet's oceans, monitoring for climate change-related risks, and mapping of other parts of our solar system.

The fast-growing critical dependence on space for national security, the global economy, and public-benefit interests makes assured space operations essential for ensuring a more free, secure, and prosperous world.

Finding 6: The US commercial space industry can increase its role in supporting national security.

The National Space Strategy[183] includes four areas of emphasis: resilience, deterrence, foundational capabilities, and more conducive domestic and international environments. It envisions improved leverage of, and support for, the US commercial industry. The Defense Space *Strategy Summary*[184] highlights that the rapidly growing commercial space industry is introducing new capabilities as well as new threats to US space operations. A main effort in this strategy is to cooperate with industry and other actors to leverage their capabilities.

"Space Policy Directive-2—Streamlining Regulations on Commercial Use of Space," provides support for the US commercial space industry.[185] In support of the overall policy of the executive branch to promote economic growth, protect national security, and encourage US leadership in space commerce, the directive requires reviews of the launch and reentry licensing for commercial space flight, the Land Remote Sensing Policy Act of 1992, the Department of Commerce's organization of its regulation of commercial space flight activities, radio frequency spectrum, and export licensing regulations.[186]

The Government Accountability Office's (GAO's) report on the Department of Defense's

[182] John J. Klein, *The Influence of Commercial Space Capabilities on Deterrence*, Center for a New American Security, March 25, 2019, accessed March 26, 2021, https://www.cnas.org/publications/reports/the-influence-of-commercial-space-capabilities-on-deterrence; US Deputy Secretary of Defense Robert Work's speech to the Satellite Industries Association, March 7, 2016, accessed March 26, 2021, https://www.defense.gov/Newsroom/Speeches/Speech/Article/696289/satellite-industries-association/; Government Accountability Office, *Military Space Systems: DoD's Use of Commercial Satellites to Host Defense Payloads Would Benefit from Centralizing Data*, July 2018, GAO-18-493, accessed March 26, 2021, https://www.gao.gov/products/gao-18-493.

[183] White House, "An America First National Space Strategy," accessed March 26, 2021, https://aerospace.csis.org/wp-content/uploads/2018/09/Trump-National-Space-Strategy.pdf.

[184] Department of Defense, *Defense Space Strategy Summary*, June 2020, accessed March 26, 2021, https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_DEFENSE_SPACE_STRATEGY_SUMMARY.PDF.

[185] Executive Office of the President, "Streamlining Regulations on Commercial Use of Space," *Federal Register*, Space Policy Directive-2 of May 24, 2018, accessed March 26, 2021, https://www.federalregister.gov/documents/2018/05/30/2018-11769/streamlining-regulations-on-commercial-use-of-space.

[186] Ibid.

(DoD's) use of commercial satellites[187] describes several potential benefits of including more responsive delivery of capabilities to space and increasing deterrence and resilience due to the larger number and distribution of commercial constellations of satellites.

Finding 6.1: Large constellations of small satellites are being developed.

The development of small satellites enables the proliferation of very large constellations of satellites. For example, several companies are currently planning constellations of communications satellites comprising an aggregate deployment of several thousand satellites in low Earth orbit (LEO). In total, the communications capacities could exceed tens of terabytes. This enables low-latency, high-bandwidth communications to any region, bringing valuable educational opportunities to underserved populations, and supporting new data-intensive communications in advanced countries.[188] Small Earth observation satellites are being deployed in constellations of hundreds of platforms by several companies. These can produce global coverage with revisit intervals ranging from minutes to hours. Several types of sensors are being deployed including electro-optical, synthetic aperture radar, and radio signal collection.[189] Companies in the United States, Europe, Russia, and China are actively pursuing these new capabilities.[190]

The ability to image any area, and to communicate with any area, will become commercially available to any individual, group, or government. Coupled with access to cloud computing and big data analytics, innovations will occur in many fields, e.g., precise, real-time weather and soil condition data for farmers to increase yield, ship tracking to aid logistics, indicators of disease spread to inform a pandemic observation network, and the like.

Large constellations may also contribute to deterrence. The larger number of platforms operating in conjunction with major military satellites may make the entire constellation more resilient.

The commercial space industry is developing satellite servicing capabilities. This helps extend the operating life of each satellite, though the ability to operate near another satellite is viewed negatively by adversaries.

Finding 6.2: There is increasing focus on cybersecurity for commercial space systems.

[187] Government Accountability Office, *Military Space Systems*, 4.

[188] Matthew A. Hallex and Travis S. Cottom, "Proliferated Commercial Satellite Constellations, Implications for National Security," *Joint Forces Quarterly* 97 (2nd Quarter 2020), accessed March 26, 2021, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-97/jfq-97_20-29_Hallex-Cottom.pdf?ver=2020-03-31-130614-940.

[189] Ibid.

[190] Ibid.

The "Space Policy Directive 5"[191] specifies the US policy for managing risks[192] to the growth and prosperity of its commercial space economy is to rely on "executive departments and agencies to foster practices within Government space operations and across the commercial space industry that protect space assets and their supporting infrastructure from cyber threats and ensure continuity of operations." Several cybersecurity principles provide the foundation for these efforts, though the directive expects space system owners and operators to be responsible for implementing cybersecurity practices and does not address enforcement actions. No timeline for the development of regulations is provided.

Finding 6.3: The UN Outer Space Treaty (OST) requires interpretation to determine when emerging commercial space platforms become targets.

The growth in the commercial satellite industry will lead to lower-cost satellites with advanced sensors, communications, on-board computation, and security capability. Over time, each small satellite, when operated in large constellations, could be more useful for military purposes.

A key determinant in the application of the UN OST to the question of whether the military can use commercial satellites is "whether the commercial satellite is actively making a contribution to military action."[193] For example, if the military is using a commercial communications satellite to relay its messages, the UN OST does not view the communications satellite as a military target. Full consideration of the treatment of dual-use commercial satellites is not settled and will evolve as more nations participate in the commercial space industry.[194] Yet, because nations like China and Russia already target (terrestrial) commercial networks as part of their computer network exploitation campaigns, it stands to reason that they will not necessarily recognize a distinction between commercial and military satellite targets.

[191] White House, Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems, presidential memoranda, September 4, 2020, accessed March 26, 2021, https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/.

[192] Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community*, April 9, 2021, accessed April 16, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf; Todd Harrison, *Space Threat Assessment 2021*, Center for Strategic and International Studies, March 31, 2021, accessed April 16, 2021, https://www.csis.org/analysis/space-threat-assessment-2021.

[193] "Practice Relating to Rule 10. Civilian Objects' Loss of Protection from Attack," ICRC IHL Database, Customary IHL, accessed March 26, 2021, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule10.

[194] P.J. Blount, "Targeting in Outer Space: Legal Aspects of Operational Military Actions in Space," *Harvard National Security Journal Features*, accessed March 26, 2021, https://harvardnsj.org/wp-content/uploads/sites/13/2012/11/Targeting-in-Outer-Space-Blount-Final.pdf; Yun Zhao, *Space Commercialization and the Development of Space Law*, Oxford University Press, July 30, 2018, accessed March 26, 2021, https://oxfordre.com/planetaryscience/view/10.1093/acrefore/9780190647926.001.0001/acrefore-9780190647926-e-42.

Finding 6.4: The development of constellations of small satellites beneficial to the military may require government support.

Commercially viable capabilities in small satellites are advancing, but may not be sufficient for some military needs at this time. For example, the resolution of an electro-optical sensor for surveilling traffic is not useful for target identification, though it may be useful for tracking troop movements. A balanced policy would require the government to focus on the more exquisite capabilities that only it can provide, while relying on the commercial sector to meet other requirements. The government can also do more to send a signal to the markets that it supports these constellations and their capabilities by purchasing commercial data and services, thereby helping to ensure a strong commercial industrial base.

Finding 6.5: Government support for commercial space activities can be strengthened.

The growth of the commercial space industry occurring in several major countries[195] requires a review of US commercial space policy[196] as the roles of government and commercial industry change in key areas. The National Aeronautics and Space Administration (NASA) is establishing a wholly commercial capability to land humans on the moon (from lunar orbit), in contrast with the prior approach of government control of human spaceflight.[197] There are efforts to consolidate and streamline the regulatory framework and organizations for US commercial space capabilities.[198] To support greater innovation and bolster US commercial space industries, recently proposed legislation identified ways to make the commercial space licensing process simpler, more timely, and more transparent.[199] These efforts attempt to balance commercial interests against the government's need to ensure the commercial space capabilities meet national security and foreign policy requirements. Such balancing may be less important as sensitive imagery becomes more available from foreign companies. To address urgent new requirements—e.g., on-orbit servicing of a space force, or continuous global observation in support of climate study, agriculture, and ocean systems—the government may require new policies to support increasing reliance on commercial space industries and new commercial space capabilities.

[195] Congressional Research Service, *Commercial Space: Federal Regulation, Oversight, and Utilization*, updated November 29, 2018, accessed March 26, 2021, https://fas.org/sgp/crs/space/R45416.pdf.

[196] American Space Commerce Free Enterprise Act of 2019, H.R. 2809 — 116th Congress (2019-2020), accessed March 26, 2021, https://www.congress.gov/bill/115th-congress/house-bill/2809.

[197] Congressional Research Service, *Artemis: NASA's Program to Return Humans to the Moon*, updated January 8, 2021, accessed March 26, 2021, https://fas.org/sgp/crs/space/IF11643.pdf.

[198] Jeff Foust, "Commerce Department seeks big funding boost for Office of Space Commerce," *SpaceNews*, February 16, 2020, accessed March 26, 2021, https://*spacenews*.com/commerce-department-seeks-big-funding-boost-for-office-of-space-commerce/.

[199] In the 115th Congress (2017-2018), the American Space Commerce Free Enterprise Act (H.R. 2809) and the Space Frontier Act of 2018 (S. 3277) include provisions to streamline the licensing process.

Approach 6: Accelerate the development and deployment of dual-use commercial satellites, including applications to Earth and space exploration.

The United States should use the emerging commercial space industry, and large constellations of small satellites, to enhance the resilience of national security space missions. This will require a deliberate strategy to guide commercial system developments, and this must be balanced with benefits that accrue to the public. The United States should, with its allies, examine how to interpret current treaties when considering the new commercial space capabilities. The United States, its allies, and private industry should implement global Earth and space observation capabilities.

Recommendation 6: Foster the development of commercial space technologies and develop a cross-agency strategy and approach to space that can enhance national security space operations and improve agriculture, ocean exploration, and climate change activities; align both civilian and military operations, and international treaties to support these uses.

Recommendation 6.1: Ensure federal investments in the commercial space industry deliver public benefits.

Congress should pass legislation that directs the Office of Science and Technology Policy (OSTP) to lead an interagency initiative that develops an economic impact assessment of existing and future government investments in the US commercial space industry, as well as a public-private investment strategy for technology innovations and operating efficiencies that will ensure subsequent benefit to the public interest. Such benefits should contribute to global access to open data sets—via a space-based Internet, space-based cloud storage and computing—of Earth observation, global health, humanitarian applications, and other areas; it should also include suitable sharing of government-funded data collections among other government programs. A cross-agency group including the National Aeronautics and Space Administration (NASA), the National Geospatial-Intelligence Agency (NGA), the Defense Advanced Research Projects Agency (DARPA), relevant federal departments, private industry, and allied nations should develop the plans and partnerships for global Earth and space observation in support of environmental security.

Recommendation 6.2: Foster commercial space technologies of strategic importance and protect these from foreign acquisition.

Congress should direct a cross-agency group including NASA and the Department of Defense to conduct a joint review [200] of dual-use commercial space technologies and capabilities that are of strategic importance to national security space missions. The scope includes communications, on-orbit storage and computing, large constellations of small platforms, sensing, space situational awareness, satellite protection, launch, and on-orbit servicing. Congress should direct a streamlined licensing process and simplify regulations where appropriate. Such dual-use technologies should be reviewed for protection from foreign acquisition by the expanded authorities of the Committee on Foreign Investment in the United States (CFIUS)[201] and by the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. The broadened role delineated by the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) enables CFIUS to review noncontrolling foreign investments in critical technologies and critical infrastructure in the US space industrial base. Congress should direct an assessment of how the FIRRMA reforms have been applied and the resulting effect.

Recommendation 6.3: Harden the security of commercial space industry facilities and space assets.

The administration should designate the commercial space industry as a critical infrastructure sector and develop a sector-specific plan for its protection. The Department of Commerce should be assigned as the Sector-Specific Agency and should work with international standards-setting groups to harden select commercial space capabilities, e.g., protect communications against cyber threats.

The cybersecurity of both military and commercial spacecraft is a growing concern. Threat actors are devoting more attention to attacking both the software/IT supply chain as well as vulnerabilities in the cyber defenses on spacecraft. Large commercial mega-constellations of small satellites are performing an increasing range of business and communications functions, yet do not necessarily conform to high cybersecurity standards. The US government does not have standards for the design of cyber-secure commercial satellites, though it is introducing self-certification programs for commercial satellite providers.

[200] National Aeronautics and Space Administration, "Memorandum of Understanding Between the National Aeronautics and Space Administration and the United States Space Force," September 2020, https://www.nasa.gov/sites/default/files/atoms/files/nasa_ussf_mou_21_sep_20.pdf. This does not address foreign acquisition of commercial space technologies of strategic importance.

[201] Congressional Research Service, *The Committee on Foreign Investment in the United States (CFIUS),* updated February 14, 2020, accessed March 26, 2021, https://fas.org/sgp/crs/natsec/RL33388.pdf.

The administration should extend the National Institute of Standards and Technology (NIST) cybersecurity maturity standards, guidelines, and best practices to the space domain, covering the space, link, ground, and user segments. The cyber-resilient design principles should consider the following: "Intrusion detection and prevention leveraging signatures and machine learning to detect and block cyber intrusions onboard spacecraft; a supply chain risk management (SCRM) program to protect against malware inserted in parts and modules; software assurance methods within the software supply chain to reduce the likelihood of cyber weaknesses in flight software and firmware; logging onboard the spacecraft to verify legitimate operations and aid in forensic investigations after anomalies; root-of-trust to protect software and firmware integrity; a tamper-proof means to restore the spacecraft to a known good cyber-safe mode; and lightweight cryptographic solutions for use in small satellites."[202]

Recommendation 6.4: Establish the conformance of emerging commercial space constellations to multinational agreements.

The United States should lead a conference to assess future developments in the commercial space industry with respect to the UN OST, the Artemis Accords,[203] and other international agreements that may be constructed. The objective is to clarify the acceptable use of commercial space assets as these become of greater use in supporting militaries.

Commercial capabilities may, over time, provide essential portions of space-based surveillance, reconnaissance, communications, refueling, data storage and processing, and maintenance. As new military space capabilities become possible, there is an increased risk that these will be interpreted as "making an effective contribution to military action" and thereby become legitimate targets. These capabilities may include imaging satellites, communications satellites, space networks, satellite maintenance vehicles, launch vehicles, and so forth. A key area to clarify is the legal and technical assessment of what qualifies as "making an effective contribution to military action" involving space technology.[204]

[202] Brandon Bailey et al., *Defending Spacecraft in the Cyber Domain*, Aerospace Corporation, November 2019, accessed March 26, 2021, https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf.

[203] National Aeronautics and Space Administration, *The Artemis Accords: Principles for Cooperation in the Civil Exploration and Use of the Moon, Mars, Comets, and Asteroids for Peaceful Purposes*, accessed March 26, 2021, https://www.nasa.gov/specials/artemis-accords/img/Artemis-Accords-signed-13Oct2020.pdf.

[204] Dr. Cassandra Steer, *Why Outer Space Matters for National and International Security*, Center for Ethics and the Rule of Law, University of Pennsylvania, January 8, 2020, accessed March 26, 2021, https://www.law.upenn.edu/live/files/10053-why-outer-space-matters-for-national-and; Jackson Nyamuya Maogoto and Steven Freeland, "Space Weaponization and the United Nations Charter Regime on Force: A Thick Legal Fog or a Receding Mist?" *International Lawyer* 41 (4) (Winter 2007): 1091–1119, http://www.jstor.org/stable/40707832, accessed March 26, 2021, https://www.law.upenn.edu/live/files/7860-maogoto-and-freelandspace-weaponizationpdf; Blount, "Targeting"; Theresa Hitchens and Colin Clark, "Commercial Satellites: Will They Be Military Targets?" *Breaking Defense*, July 16, 2019, accessed March 26, 2021, https://breakingdefense.com/2019/07/commercial-satellites-will-they-be-military-targets/.

Recommendation 6.5: Develop space technologies for mega-constellations of satellites that support monitoring the entire planet pervasively and persistently, at high resolution and communicate the information in near-real time.

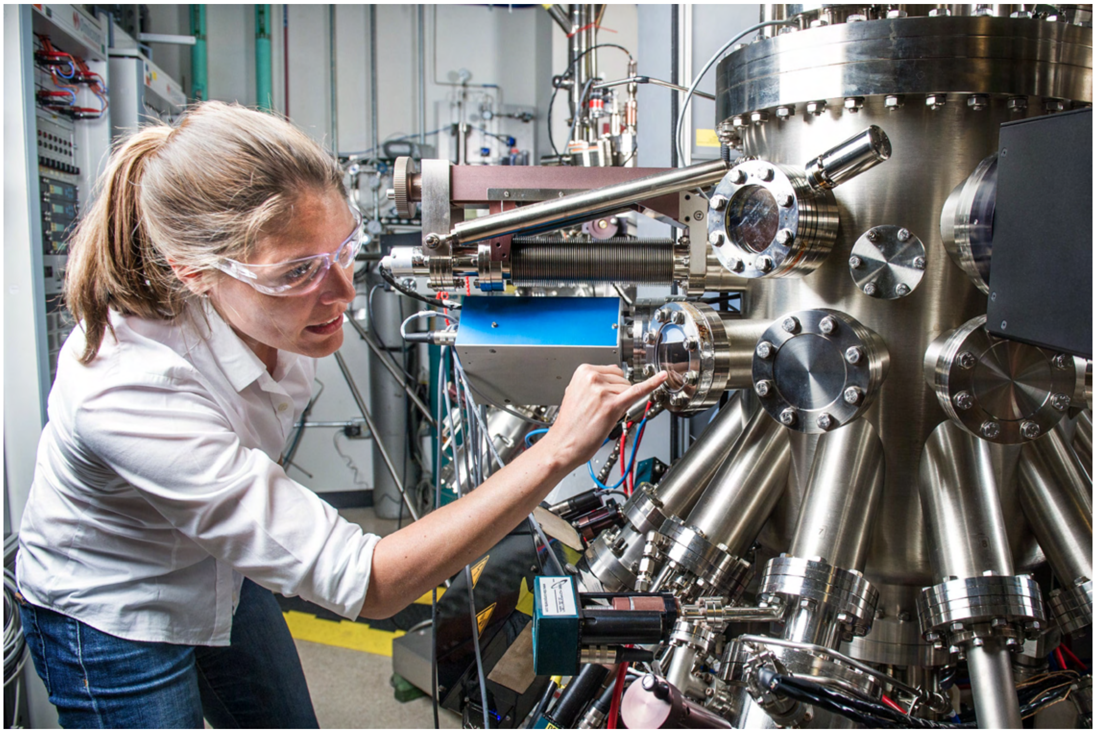
The administration should develop autonomous space operations technologies for large-scale constellations. This program, led by the DoD, NASA, and other elements of the national security space enterprise, would use AI technologies to minimize or eliminate human requirements for satellite control, information collection, and information analysis; and increase the speed of the information-to-decision loop.

The administration should encourage commercial space companies to develop cost-effective technologies that increase the survivability of commercial satellites as the operating regions become more crowded or contested. This may enable commercial satellites to operate in a greater variety of conditions, thereby providing expanded value to the United States.

The administration should develop and conduct Challenge Prizes funding opportunities for autonomous satellite operations on single platforms, i.e., for applications where highly capable satellites autonomously manage their own complex taskings, and also work as part of a large collection of similarly autonomous satellites.

The administration should use the model of the NASA Tipping Point solicitation to develop the capability to continuously monitor the world's oceans—in particular, using space-based sensors—for the impact of climate change and other issues of global importance. This program would be jointly managed by NASA, NSF, and DARPA with collaborations from the European Union (EU) and other participants. This multiyear initiative would help establish a global, real-time Earth oceans observation network and the supporting autonomous control, communications, and data analytics capabilities. In addition to space technologies, this program could also support the development of surface and underwater vehicles to perform this function. The Department of State should address the treaty implications of large numbers of remotely-piloted and autonomous surface and underwater vehicles and develop new international agreements where needed.

Chapter 7. Future of Work



A scientist at the National Renewable Energy Laboratory in Colorado uses a semiconductor growing system at the Solar Energy Research Facility.

SCIENCE IN HD VIA UNSPLASH

While this report has focused on the technological changes that will impact geopolitics over the next decade, the recommendations contained within will be meaningless if the United States and allied nations ignore the most important ingredient in the success or failure of all endeavors: people. Developing a digitally fluent and resilient workforce that can meet the challenges of the GeoTech Decade will require private and public sectors to pursue several approaches. These include a broadened view of technical competencies and how they are acquired, improved alignment of skills and job requirements, incentives for employer-based training, and data collection to help assess the effectiveness of these investments and their effects on workers. Ensuring that people, especially people from underrepresented communities, are not left behind by the advance of technology—and that societies have the skilled workforces they need to innovate and prosper—will determine whether the GeoTech Decade lives up to its ambition.

From artificial intelligence (AI) to quantum computing, and for applications ranging from augmented reality to smart cities and communities,[205] the technologies that will shape

[205] Smart Cities and Communities Act of 2019, H.R. 2636 — 116th Congress (2019-2020), accessed March 26, 2021, https://www.congress.gov/116/bills/hr2636/BILLS-116hr2636ih.pdf.

the GeoTech Decade require specialized investments in the US workforce.[206] Shifting from the "findings and recommendations" format of the previous chapters, this closing chapter discusses key areas needing greater focus and investment from businesses, governments, educational institutions, and stakeholder organizations, as follows.

Create the Workforce for the GeoTech Decade

Recognize the diverse competencies that characterize skilled technical workers

Diverse competencies include academic credentials, technical competencies in an industry, and technical competencies in a specific occupation, plus "soft skills" that make for reliable and collegial employees.[207] Job descriptions should consider the value of all sources of relevant experience and ability.

Communicate the breadth of pathways for gaining skilled technical work

Given the current focus on a college degree being a prerequisite to desirable, skilled technical jobs, the workforce should be better informed about the variety of skilled technical occupations, the different ways of acquiring credentials, e.g., college certificates, professional certifications, professional licenses, and digital badges and how such credentials allow more points of entry into desired occupations.

Strengthen skilled technical training and education

Secondary school: Career and technical education (CTE) programs[208] enable the acquisition of STEM education combined with work experience that teaches technical skills relevant to specific professions. CTE programs can be enhanced through active participation and guidance provided by representatives from local businesses. This could help ensure that the skills training is better matched with employer needs and requirements. The P-TECH program, now operating schools in eleven US states, Australia, Morocco, and Taiwan, is another model for building regional workforces with the needed technical skills and for providing underserved youths with opportunities for gaining relevant technical skills.[209]

[206] National Academies of Sciences, Engineering, and Medicine, *Building America's Skilled Technical Workforce* (Washington, DC: National Academies Press, 2017) accessed April 16, 2021, http://nap.edu/23472; Mark Warner, "Part II. Investing in Workers," Medium, February 8, 2021, accessed April 16, 2021, https://senmarkwarner.medium.com/ii-investing-in-workers-e7e9a09ff24c.

[207] National Academies of Sciences, Engineering, and Medicine, *Building America's Skilled*.

[208] Bri Stauffer, "What Is Career & Technical Education (CTE)?" Applied Educational Systems, February 4, 2020, accessed April 16, 2021, https://www.aeseducation.com/blog/career-technical-education-cte.

[209] "What is P-TECH all about?" website homepage accessed April 16, 2021, https://www.ptech.org/.

Post-secondary school: There are 936 public community colleges in the United States,[210] representing a nationwide resource for improving the technical skills of the current and future workforce. According to a Community College Resource Center analysis, "6.7 million students were enrolled at community colleges in fall 2017, and nearly 10 million students enrolled at a community college at some point during the 2017-18 academic year. Yet, the overall percent of community college enrollees in 2014 that completed a college degree at a four-year institution within six years is 17 percent."[211] Increasing this completion rate through financial incentives and investments could increase the number and qualifications of the technically skilled workforce in the United States.

Non-college credentials: The value to the worker and the employer of non-college degree certification programs—apprenticeships, certifications, certificate programs—could be improved by better linking them to established, defined technical workforce competencies. Improved standards and data on the effectiveness of these credentials will help workers and employers determine the value of these credentials and enable more informed choices for skills training.

Alternative sources of skilled workers: A recent study[212] examined the prevailing practice of a four-year college degree being a prerequisite for skilled jobs. The analysis identified large populations of workers with suitable skills but who did not have a college degree. Of these, the analysis showed that twenty-nine million have skills that would enable them to transition to an occupation with a significantly higher wage. These results suggest that job descriptions should be carefully specified so as to reach the largest qualified talent pool.

Better align employer-based training with needs

Business incentives: Incentives for employers to invest in improving workforce technical skills should help a company remain competitive. The investments would align the employer's needs for technically skilled workers and the training and education that is offered. One approach could be based on tax incentives for increasing investment in workforce skill development to increase productivity."[213]

[210] "Number of community colleges in the United States in 2021, by type," Statista, accessed April 16, 2021, https://www.statista.com/statistics/421266/community-colleges-in-the-us/.

[211] "Community College FAQs," Community College Research Center, Teachers College, Columbia University, accessed April 16, 2021, https://ccrc.tc.columbia.edu/Community-College-FAQs.html.

[212] Peter Q. Blair et al., "Searching for STARs: Work Experience as a Job Market Signal for Workers without Bachelor's Degrees," National Bureau of Economic Research, March 2020, accessed April 16, 2021, https://www.nber.org/papers/w26844.

[213] Warner, "Part II. Investing in Workers."

Technology development and training: Workforce organizations can play a role in effectively communicating, between employers and the workforce, issues concerning needed technical skills and the mechanisms and policies being used to manage these requirements. To accelerate identifying and acquiring future technical skills needed by the workforce, technology development programs could also create a training program for the skills associated with using the new technology in a product. This can shorten the link between technology development and the training of workers.

Acquire and analyze human capital development and management data

Human capital development and management data should address projections of the supply and demand for workers according to categories of technical skills, results of the search and hiring process, and how well the employer's needs were satisfied. The data also should inform how well the training policies provided equitable access to skills training across the workforce.

These data should enable analyses of the expected value of different options for skills education and training for workers, the return on the investment of workforce training for businesses, and options for adjusting workforce training policies.

Foster lifelong learning

The pace at which advanced technology is changing the workplace and the skills needed to maintain a competitive economy makes lifelong learning imperative. Individuals should be able to guide their training and education throughout their working years.

To accomplish this on a national scale will require effort to craft incentives that motivate individuals to embrace this approach. Important elements may involve information on the value of continuing educational programs and the job opportunities that are enabled, funding mechanisms to lower the cost to the individual, and strategies developed with businesses that specify how continuing learning enhances an individual's work prospects.

To guide individual choices, new tools can facilitate gathering and synthesizing the complex array of information on skills, occupations, training opportunities, and assessments of their value. The tools can also help the individual identify and secure funding from available sources, and help government funding sources be applied efficiently to this long-term challenge.

Equitable Access to Opportunity

The United States needs to ensure equitable access to opportunity during the GeoTech Decade. From access to affordable broadband to digital literacy, governments and the private sector need to make significant investments and work together to reduce barriers to full participation in the economy.

Access to affordable, high-speed Internet and devices to use it

Ensuring that all people can participate in the GeoTech Decade requires a commitment to equitable access to affordable, high-speed Internet. Millions do not have high-speed broadband, particularly in rural areas.[214] What is more, many with access to high-speed broadband are still unable to afford the high cost of Internet and the devices needed to access it.[215] Lack of access and affordability perpetuates systemic inequities.

While Congress has made significant investments in broadband since the onset of the COVID-19 pandemic, more remains to be done. The Emergency Broadband Benefit Program has helped low-income households afford broadband during the pandemic.

Acquiring digital literacy

Digital literacy, the ability to find, evaluate, utilize, and create information using digital technology, is becoming an essential skill for every individual. Digital literacy is an important element in eliminating a digital divide among nations and within a society. It complements affordable, high-speed Internet access by enabling people to develop and communicate local content, to communicate their issues and concerns, and to help others understand the context in which these issues occur.

[214] Federal Communications Commission, *2020 Broadband Deployment Report*, April 24, 2020, accessed April 16, 2021, https://docs.fcc.gov/public/attachments/FCC-20-50A1.pdf.

[215] Tom Wheeler, *5 steps to get the internet to all Americans COVID-19 and the importance of universal broadband*, Brookings Institution, May 27, 2020, accessed April 16, 2021, https://www.brookings.edu/research/5-steps-to-get-the-internet-to-all-americans/.

Conclusion

The increasing capabilities and availability of data and new technologies change how nations remain competitive and secure. In the coming GeoTech Decade, data and technology will have a disproportionate impact on geopolitics, global competition, and global opportunities for collaboration as new capabilities may eliminate a technical advantage or may enable new processes superior to current methods. The United States and like-minded nations must be able to adapt and demonstrate effective governance, at faster speeds, in employing data and new technologies to promote a more secure, free, and prosperous world.

In 1945, Vannevar Bush, director of the Office of Scientific Research and Development, transmitted a report, *Science – the Endless Frontier*,[216] with the goal of answering a few key questions asked by then-President Franklin D. Roosevelt in November 1944. In the report, Bush elaborated:

> "With particular reference to the war of science against disease, what can be done now to organize a program for continuing in the future the work which has been done in medicine and related sciences?
>
> "What can the Government do now and in the future to aid research activities by public and private organizations?
>
> "Can an effective program be proposed for discovering and developing scientific talent in American youth so that the continuing future of scientific research in this country may be assured on a level comparable to what has been done during the war?"

Among its recommendations, the 1945 report called for the creation of the National Research Foundation. Bush concluded, noting the importance of action by Congress:

> "Legislation is necessary. It should be drafted with great care. Early action is imperative, however, if this nation is to meet the challenge of science and fully utilize the potentialities of science. On the wisdom with which we bring science to bear against the problems of the coming years depends in large measure our future as a nation."

Now, almost seventy-six years later, the GeoTech Commission similarly seeks to promote freedom and security through initiatives that employ data and new technologies to amplify the ingenuity of people, diversity of talent, strength of democratic

[216] *Science — The Endless Frontier*, a report to the president by Vannevar Bush, director of the Office of Scientific Research and Development, July 1945, accessed March 26, 2021, https://nsf.gov/od/lpa/nsf50/vbush1945.htm.

values, innovation of companies, and the reach of global partnerships.

There are several areas where data and technology can help, or hinder, the achievement of these goals:

- Communications and networking, data science, cloud computing
- Artificial intelligence, distributed sensors, edge computing, the Internet of Things
- Biotechnologies, precision medicine, genomic technologies
- Space technologies, undersea technologies
- Autonomous systems, robotics, decentralized energy methods
- Quantum information science, nanotechnology, new materials for extreme environments, advanced microelectronics

To maintain national and economic security and competitiveness in the global economy, the United States and its allies must continue to be preeminent in these key areas, and must achieve trustworthy and assured performance of the digital economy and its infrastructure. The GeoTech Commission provided recommendations in the following seven areas where the United States and like-minded nations must succeed:

- **Global science and technology leadership**
- **Secure data and communications**
- **Enhanced trust and confidence in the digital economy**
- **Assured supply chains and system resiliency**
- **Continuous global health protection and global wellness**
- **Assured space operations for public benefit**
- **Future of work**

The report's recommendations embody several ideals. First, work to ensure the benefits of new technologies reach all sectors of society. Second, define protocols and standards for permissible ways to develop and use technologies and data, consistent with the norms of the United States and like-minded nations. Third, guide technology cooperation and sharing with nondemocratic nations based on respecting democratic values.

Just as Vannevar Bush urged in 1945, the United States must create new ways to develop and employ future critical and emerging technologies at speed, cultivate the needed human capital, and establish norms for international cooperation with nations. Such creation requires important action by Congress and the new administration to ensure that the United States has the wisdom with which to apply science to the challenges and opportunities of the coming years. If enacted, the report's recommendations will enable the United States and like-minded nations to employ data capabilities and new technologies intentionally to promote a freer, more secure, and more prosperous world.

Commission on the Geopolitical Impacts of New Technologies and Data
Be Bold
Be Brave
Be Benevolent

Appendix A. Additional Readings on Identifying and Countering Online Misinformation

Misinformation has existed for most of human history and has been wielded to influence geopolitics. Johns Hopkins University's Sheridan Libraries defines misinformation as follows:

> "'Misinformation' is defined as the action of misinforming or the condition of being misinformed; or erroneous or incorrect information. Misinformation differs from propaganda in that it always refers to something which is not true. It differs from disinformation in that it is 'intention neutral'; that is, misinformation is not deliberate, just wrong or mistaken. One of the most popular forms of misinformation on the Internet is the passing along of 'urban legends.' Urban legends are fabricated or untrue stories that are passed along by sincere people who believe them, and then 'inform' others."[217]

Recent advances with the Internet and social media have provided a way to propagate misinformation and disinformation more rapidly and democratized the ability for both individuals and automated programs ("bots") to accelerate their propagation online. As digital technologies have become democratized, so too has the ability for others to use these technologies to shape narratives in ways that were not readily available thirty or forty years ago. As we navigate the GeoTech Decade ahead, we will need to identify solutions to sift through all the information produced and shared online. Listing in chronological order from 2015 to 2021, these five readings represent scholarly research on this evolving topic area.

[217] "Evaluating Information: Information and Its Counterfeits: Propaganda, Misinformation and Disinformation," Sheridan Libraries, Johns Hopkins, https://guides.library.jhu.edu/evaluate/propaganda-vs-misinformation.

1. This Is Why We Can't Have Nice Things: Mapping the Relationship between Online Trolling and Mainstream Culture

Author: Whitney Philips

Publication date: 2015

Publisher: MIT Press

> Excerpt from the publication:
>
> "Trolls also fit very comfortably within the contemporary, hyper-networked digital media landscape. Not only do they put Internet technologies to expert and highly creative use, their behaviors are often in direct (if surprising) alignment with social media marketers and other corporate interests. Furthermore, they are quite skilled at navigating and in fact harnessing the energies created when politics, history, and digital media collide. In short, rather than functioning as a counterpoint to 'correct' online behavior, trolls are in many ways the grimacing poster children for the socially networked world."

Link: https://www.jstor.org/stable/j.ctt17kk8k7

2. Media Manipulation and Disinformation Online

Authors: Alice Marwick and Rebecca Lewis

Publication date: May 15, 2017

Publisher: Data & Society Research Institute

> Excerpt from the report:
>
> "'Trolling' developed in tandem with the internet. Initially, the term 'troll' described those who deliberately baited people to elicit an emotional response. Early trolls posted inflammatory messages on Usenet groups in an attempt to catch newbies in well-worn arguments. During the '00s, this motivation became known as the 'lulz': finding humor (or LOLs) in sowing discord and causing reactions. Trolls have a history of manipulating the media to call out hypocrisies and hysterias, learning early on how to target public figures and organizations to amplify their efforts through mainstream media. They have often claimed to be apolitical and explained their use of shocking (often racist or sexist) imagery as merely a convenient tool to offend others. Trolling can refer to relatively innocuous pranks, but it can also take the form of more serious behaviors. Trolling can include 'mischievous activities where the intent is not necessarily to cause distress' or it can seek to 'ruin the reputation of individuals and organizations and reveal embarrassing or personal information.' In practice, however, trolling has grown to serve as an umbrella term which encompasses a wide variety of asocial internet behaviors."

Link: https://www.datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf

3. Source Hacking: Media Manipulation in Practice

Authors: Joan Donovan and Brian Friedberg

Publication date: September 4, 2019

Publisher: Data & Society Research Institute

> Excerpt from the report:
>
> "In recent years there has been an increasing number of online manipulation campaigns targeted at news media. This report focuses on a subset of manipulation campaigns that rely on a strategy we call source hacking: a set of techniques for hiding the sources of problematic information in order to permit its circulation in mainstream media. Source hacking is therefore an indirect method for targeting journalists—planting false information in places that journalists are likely to encounter it or where it will be taken up by other intermediaries.
>
> "Across eight case studies, we identify the underlying techniques of source hacking to provide journalists, news organizations, platform companies, and others with a new vocabulary for describing these tactics, so that terms such as 'trolling' and 'trending' do not stand in for concerted efforts to pollute the information environment. In this report, we identify four specific techniques of source hacking:
>
> - Viral Sloganeering: repackaging reactionary talking points for social media and press amplification
> - Leak Forgery: prompting a media spectacle by sharing forged documents
> - Evidence Collages: compiling information from multiple sources into a single, shareable document, usually as an image
> - Keyword Squatting: the strategic domination of keywords and sockpuppet accounts to misrepresent groups or individuals
>
> "These four tactics of source hacking work because networked communication is vulnerable to many different styles of attack and finding proof of coordination is not easy to detect. Source hacking techniques complement each other and are often used simultaneously during active manipulation campaigns. These techniques may be carefully coordinated but often rely on partisan support and buy-in from audiences, influencers, and journalists alike."

Link: https://apo.org.au/node/257046

4. Deepfakes and Cheap Fakes: The Manipulation of Audio and Visual Evidence

Authors: Britt Paris and Joan Donovan

Publication date: September 18, 2019

Publisher: Data & Society Research Institute

> Excerpt from the publication:
>
> “The first widely-known examples of amateur, AI-manipulated, face swap videos appeared in November 2017. Since then, the news media, and therefore the general public, have begun to use the term ‘deepfakes’ to refer to this larger genre of videos—videos that use some form of deep or machine learning to hybridize or generate human bodies and faces. News coverage claims that deepfakes are poised to assault commonly-held standards of evidence, that they are the harbingers of a coming ‘information apocalypse.’ But what coverage of this deepfake phenomenon often misses is that the ‘truth’ of audiovisual content has never been stable—truth is socially, politically, and culturally determined.
>
> “Deepfakes which rely on experimental machine learning represent one end of a spectrum of audio-visual (AV) manipulation. The deepfake process is both the most computationally-reliant and also the least publicly accessible means of creating deceptive media. Other forms of AV manipulation –‘cheap fakes’ –rely on cheap, accessible software, or no software at all. Both deepfakes and cheap fakes are capable of blurring the line between expression and evidence. Both can be used to influence the politics of evidence: how evidence changes and is changed by its existence in cultural, social, and political structures.”

Link: https://datasociety.net/wp-content/uploads/2019/09/DS_Deepfakes_Cheap_FakesFinal-1-1.pdf

5. 'Stop the Presses? Moving from Strategic Silence to Strategic Amplification in a Networked Media Ecosystem'

Authors: Joan Donovan and Danah Boyd

Publication date: September 29, 2019

Publisher: *American Behavioral Scientist* (65) (2): 333–350, SAGE Publications

> Excerpt from the publication:
>
> "In a media ecosystem besieged with misinformation and polarizing rhetoric, what the news media chooses not to cover can be as significant as what they do cover. In this article, we examine the historical production of silence in journalism to better understand the role amplification plays in the editorial and content moderation practices of current news media and social media platforms. Through the lens of strategic silence (i.e., the use of editorial discretion for the public good), we examine two U.S.-based case studies where media coverage produces public harms if not handled strategically: White violence and suicide. We analyze the history of journalistic choices to illustrate how professional and ethical codes for best practices played a key role in producing a more responsible field of journalism. As news media turned to online distribution, much has changed for better and worse. Platform companies now curate news media alongside user generated content; these corporations are largely responsible for content moderation on an enormous scale. The transformation of gatekeepers has led an evolution in disinformation and misinformation, where the creation and distribution of false and hateful content, as well as the mistrust of social institutions, have become significant public issues. Yet it is not just the lack of editorial standards and ethical codes within and across platforms that pose a challenge for stabilizing media ecosystems; the manipulation of search engines and recommendation algorithms also compromises the ability for lay publics to ascertain the veracity of claims to truth. Drawing on the history of strategic silence, we argue for a new editorial approach—'strategic amplification'—which requires both news media organizations and platform companies to develop and employ best practices for ensuring responsibility and accountability when producing news content and the algorithmic systems that help spread it."

Link: https://journals.sagepub.com/doi/abs/10.1177/0002764219878229

Appendix B. Improving the Software Supply Chains and System Resiliency for the US Government

Overview

Since FireEye's public disclosure[218] on December 8, 2020, of the theft of its penetration testing toolkit, story after story has revealed the staggering breadth of a comprehensive cyber breach centered on SolarWinds' Orion network monitoring software. State-sponsored adversaries compromised the widely used program in its build stages, allowing them to infiltrate over eighteen thousand commercial and government targets, including Intel, Microsoft, California state hospitals,[219] the National Nuclear Security Administration,[220] and dozens[221] of federal, state, and local government agencies, reportedly with the goal of extracting valuable intelligence.

The SUNBURST event[222] is a case study in software supply chain attacks, in which attackers compromise targets by exploiting vulnerabilities not just within target networks and infrastructure themselves, but in the programs and code that those systems rely on, either through programmed dependency or purchase and acquisition. Attackers are migrating[223] toward the most vulnerable points in complex digital supply chains, employing attacks resembling the SUNBURST event: compromised updates and installers used as distribution networks to create entry points into sensitive systems,

[218] Kevin Mandia, "FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community," FireEye, December 08, 2020, accessed March 26, 2021, https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html.

[219] Hautala, "SolarWinds hackers accessed DHS acting secretary's emails."

[220] Bertrand and Wolff, "Nuclear weapons agency."

[221] Satter, "U.S. cyber agency."

[222] SolarWinds' Orion program was not the only vector pursued by attackers. However, it has received the most public scrutiny so far and is the purest supply chain component of the attack. As such, the expansive intelligence gathering operation is, throughout this appendix, referred to as the SUNBURST campaign, to acknowledge the central role of the most notorious piece of associated malware, with full acknowledgement that the nomenclature oversimplifies an extraordinarily sophisticated event involving many vectors, which were not always related.

[223] Sonatype, 2020 State of the Software Supply Chain Report, accessed March 26, 2021, https://www.sonatype.com/campaign/wp-2020-state-of-the-software-supply-chain-report.

perpetrated by state-backed attackers with deeply sophisticated methods. Data from the Atlantic Council's Breaking Trust report[224] found thirty-six attacks in recent years bearing similar characteristics. Attackers pick at the weak points on software supply chains and pose a critical threat to national security; government procedures, born out of traditional processes designed for the acquisition of physical systems,[225] are ill-suited to moderate the dynamic and complex software ecosystem.

The software supply chain provides remarkable return on investment for attackers, where successfully undermining one update or installer can provide attackers access to thousands of systems and millions of machines. The software supply chains are increasingly leveraged in a cyber espionage contest. State-backed actors work to compromise widely used and deeply permissioned software to seek useful intelligence and intellectual property. In this realm, deterrence is difficult, capabilities wide-ranging, and precise, public attribution of the most successful breaches challenging, both technically and, sometimes more importantly, politically. It is not simply a story of compromised products but also the insecure configurations within vulnerable networks backed by limited staff resources and burdened by immense complexity and rapid change. The problem as manifested in federal acquisition practices is not primarily technological or geopolitical, but organizational. Such attacks may further erode the United States' competitive edge and compromise its national security.

This appendix focuses on the main lines of effort that the US government must undertake to improve the security of software supply chains, informed by its current shortcomings: improving baseline requirements, empowering agencies to implement basic supply chain risk management (SCRM) practices, reframing software security as a holistic undertaking, better coordinating between agencies and network types, and improving private sector involvement. This appendix focuses specifically on government acquisition processes and certification policies, addressing direct national security concerns. It does not recommend specific legislation but rather the end states towards which any reforms must strive.

[224] Trey Herr et al., "Breaking trust: The Dataset," Cyber Statecraft Initiative, Atlantic Council, accessed March 26, 2021, https://www.atlanticcouncil.org/resources/breaking-trust-the-dataset/.

[225] J. Michael McQuade et al., *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage*, Defense Innovation Board, May 3, 2019, accessed March 26, 2021, https://media.defense.gov/2019/May/01/2002126689/-1/-1/0/SWAP%20COMPLETE%20REPORT.PDF.

Lines of Improvement

Meet the Baselines: The December 2020 Government Accountability Office (GAO) report, *Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*,[226] on software/IT supply chain risk management (SCRM) implementation found that, of twenty-three studied federal civilian agencies, no agency had implemented the seven foundational practices. Fourteen had not implemented any. Most agencies cited either insufficient guidance, inadequate bandwidth and staff power, or the overwhelming burden of implementation. Some delegated the task to internal bureaus and initiatives, while others preferred to deal with software/IT supply chain challenges as they came. The systemic failure to comply with "Office of Management and Budget (OMB) Circular No. A-130, Managing Information as a Strategic Resource," the main directive examined by the GAO report, indicates a clear need for centralized assistance to prioritize and address the known shortcomings of federal agencies' software/IT supply chain practices. Such an effort must balance helping agencies establish and formalize their SCRM practices with leveraging their knowledge of their own networks and practices.

Mature the Baselines: The many federal guidance documents on software SCRM—OMB Circular A-130, the Department of Defense's (DoD's) new *Cybersecurity Maturity Model Certification (CMMC)*, the Federal Information Security Modernization Act (FISMA), the DoD Information Network (DoDIN) Approved Products List (APL), the Federal Risk and Authorization Management Program (FedRAMP), and more—all draw on a common set of security guidelines laid out by the National Institute of Standards and Technology (NIST), mainly in Special Publications 800-53 for agencies and 800-171 for vendors managing Controlled Unclassified Information (CUI), as well as several other 800 series publications. These guidelines apply to the agencies assuming the risk of acquired products, the vendors providing them, and the products themselves. The NIST Cybersecurity Framework, far from providing specific recommendations, is more akin to a static checklist of best practices in thinking about cybersecurity. For example, SolarWinds' Orion program was on DoDIN's APL,[227] was Common Criteria certified,[228] had Federal Information Processing Standards (FIPS) 140-2 compliant modules and modes,[229] and so on. The standards were insufficient to protect against an extremely sophisticated threat. More concrete, verifiable vendor practices and product

[226] Government Accountability Office, *Information Technology: Federal Agencies Need.*

[227] "DoDIN Approved Products List," DISA, accessed March 26, 2021, https://aplits.disa.mil/processAPList.action.

[228] "SolarWinds Orion Suite v3.0 Added to DoDIN APL," SolarWinds, accessed March 26, 2021, https://www.solarwinds.com/federal-government/solution/dodin-apl; technically they are certified. However, they were only certified to Evaluation Assurance Level AL 2+ which is low; the highest level is 7. EAL 2+ is insufficient to trust a product with administrative credentials to the network.

[229] "Documentation for Orion Platform: Enable FIPS for Orion Platform products," SolarWinds, accessed March 26, 2021, https://documentation.solarwinds.com/en/Success_Center/orionplatform/content/core-enabling-fips-sw1508.htm.

characteristics are necessary, and such predictability will also ease the burden of compliance on vendors.

- Assume Compromise and Mitigate: Even the most rigorous checks will fail to prevent every incursion, especially by the most capable, state-backed threat actors. With the assumption that breach is inevitable, it is crucial that agency practices mitigate the spread of breaches and impose costs on attackers. Post-compromise lateral movement was a significant part of the SUNBURST incident, leveraging vulnerabilities in Security Assertion Markup Language (SAML) tokens[230] and Azure Active Directory configurations. Agencies, where possible, must implement best network practices such as least privileged access, whitelisting, and authentication auditing to reduce the blast radius of compromised software.
- Monitor Compliance Continuously: While NIST 800-53 and 800-171 provide some guidance on the systems-level continuous monitoring of security controls within vendors and agencies (with more in-depth discussions in NIST 800-137), most acquisition systems are still based on periodic review over a long time frame. FISMA compliance is reviewed annually,[231] CMMC incorporates annual reviews[232] and is generally valid for three years, FedRAMP[233] incorporates both annual assessments and monthly reports, and DoDIN APL[234] listing is valid for three years with the option to extend by another three. Such periodicity, even if supplemented with review of patches and ongoing assessment, is out of step with the rapid dynamism of software development, and where possible, agencies should implement and automate compliance monitoring continuously. The aforementioned programs do incorporate update reviews and continuous practices, but the full extent to which they are used is unclear, and the success of their implementation is insufficient. The burden of this adjustment further highlights the need to centralize expertise and lean on automation.

[230] Jai Vijayan, “SolarWinds Campaign Focuses Attention on ‘Golden SAML’ Attack Vector,” DARKReading, December 22, 2020, accessed March 26, 2021, https://www.darkreading.com/attacks-breaches/solarwinds-campaign-focuses-attention-on-golden-saml-attack-vector/d/d-id/1339794.

[231] “Federal Information Security Modernization Act,” Cybersecurity and Infrastructure Security Agency, accessed March 26, 2021, https://www.cisa.gov/federal-information-security-modernization-act.

[232] Office of the Under Secretary of Defense (Acquisition and Sustainment), *Cybersecurity Maturity Model Certification (CMMC)*, Version 1.02, March 18, 2020, Department of Defense, accessed March 26, 2021, https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf.

[233] “Frequently Asked Questions,” Federal Risk and Authorization Management Program, accessed March 26, 2021, https://www.fedramp.gov/faqs/.

[234] Defense Information Systems Agency, “Department of Defense Information Network (DoDIN) Approved Products List (APL) Process Guide,” Version 2.5, July 2017, accessed March 26, 2021, https://www.disa.mil/-/media/Files/DISA/Services/UCCO/APL-Process/APL_Process_Guide.pdf.

Adjust to the Digital Ecosystem: Federal acquisition processes have long been criticized as poor fits for software because of the unique dynamism of software and its life cycle[235] as compared to traditional products. Moreover, as government continues to acquire and iterate more software, the magnitude of revamping policies and applying new protocols to old purchases grows increasingly expensive. The following can help government adjust to digitally oriented practices.

- Prioritize and Secure: Trends[236] in software supply chain attacks indicate a clear attacker preference: leveraging highly privileged, widely used programs. The Orion program is used by information technology (IT) departments to monitor network traffic, giving it significant access to host systems and allowing attackers to disguise the data they exfiltrated within the program's regular network traffic. Similar software compromised in state-linked incursions—CCleaner (twice),[237] Able Desk,[238] EVLog,[239] Vietnamese government digital signature packages,[240] and so on—offer deep system access and a broad (and sometimes contractually or legally obligated) userbase. The method of compromising updates and installers gives attackers access to a vast number of potential valuable targets—eighteen thousand customers in the SUNBURST campaign. Not all government-used software requires the same rigor in security, and applying controls equally to all programs is time consuming and expensive. Agencies should identify what systems and programs would be most fruitful for attackers to compromise and prioritize securing those soft spots and mitigating the consequences of their compromise first, informed in part by the threat profiles of known incursions. Such an approach also presents the opportunity for offensive components of government to provide valuable intelligence on the attack surfaces of partner agencies and help guide

[235] McQuade et al., *Software Is Never Done*.

[236] "Breaking Trust," Cyber Statecraft Initiative, Atlantic Council, website homepage accessed March 26, 2021, https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/breaking-trust/.

[237] Lily Hay Newman, "Inside the Unnerving Supply Chain Attack That Corrupted CCleaner," *Wired*, April 17, 2018, accessed March 26, 2021, https://www.*wired*.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/; Lindsey O'Donnell, "Avast Network Breached As Hackers Target CCleaner Again," threatpost, October 21, 2019, https://threatpost.com/avast-network-breached-as-hackers-target-ccleaner-again/149358/.

[238] Mathieu Tartare, "Operation StealthyTrident: corporate software under attack," welivesecurity, December 10, 2020, accessed March 26, 2021, https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/.

[239] "Kingslayer – A Supply Chain Attack," RSA, accessed March 26, 2021, https://www.rsa.com/en-us/offers/kingslayer-a-supply-chain-attack.

[240] Ignacio Sanmillan and Matthieu Faou, "Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia," welivsecurity, December 17, 2020, accessed March 26, 2021, https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/.

these efforts. The National Security Agency's (NSA's) public disclosure[241] of a critical vulnerability to Microsoft in January 2020 highlights the fact that US offensive elements are looking for the same exploitable flaws that defenders seek to close—in this case, a compromise in the cryptography of a Microsoft library used to verify code-signing and encrypted channels. The Vulnerabilities Equities Process (VEP), in particular, has unrealized potential to support national and industry defense with the resources of the nation's premiere offensive capabilities,[242] and information sharing throughout government can be improved to the same ends.

- Define and Extend the Boundaries of Security: The traditional concept of an acquired product as one that can be assessed, secured, and then deployed maps poorly onto software, which is frequently updated and iterated post-deployment, and the desired requirements of which are changed during development, both to the benefit of users. The security of shipped code can only be maintained through the security practices of its maintainers. The prevalence of compromised updates as an attack vector in software supply chain incidents illustrates that the security of a network extends all the way down to the security of the developer workstations maintaining its components. Thus, an emphasis on even the most basic cyber hygiene practices is needed, as several of the previously mentioned supply chain attacks can be traced back ultimately to insecure developer workstations (e.g., CCleaner) and poor cyber hygiene. Agencies must broaden their view of security in this dynamic environment and increase their rigor in verifying updates to already deployed software.

- Audit Networks Continuously: In line with the previously discussed Monitor Compliance Continuously section, compromise detection relies on measurements of network behavior and interaction. SCRM is ultimately an exercise in complexity management, and self-knowledge is critical to characterizing that complexity. In the case of SUNBURST, network monitoring and auditing could have detected[243] mismatches in login and authentication requests in Azure Active Directories or picked up on the creation of new trust entities, alerting victims to attacker behavior. It is important to note that these Golden SAML

[241] National Security Agency, "Patch Critical Cryptographic Vulnerability in Microsoft Windows, Clients and Servers," Cybersecurity Advisory, January 14, 2020, accessed March 26, 2021, https://media.defense.gov/2020/Jan/14/2002234275/-1/-1/0/CSA-WINDOWS-10-CRYPT-LIB-20190114.PDF.

[242] William Loomis and Stewart Scott, "A Role for the Vulnerabilities Equities Process in Securing Software Supply Chains," *Lawfare*, January 11, 2021, accessed March 26, 2021, https://www.lawfareblog.com/role-vulnerabilities-equities-process-securing-software-supply-chains.

[243] Sygnia, "Detection and Hunting of Golden SAML Attack," December 2020, accessed March 26, 2021, https://www.sygnia.co/golden-saml-advisory.

tactics were known as early as 2017,[244] but also that they were not the only means of exploiting Identity and Access Management systems in Microsoft's cloud architecture. Continual assessment of network metrics can detect aberrant behavior and decrease the length of time that a compromise goes undetected. Agencies should implement such continual assessments where possible and require the same of vendors, with an eye toward identifying what trip wires are most useful to security assurance.

Coordinate among Agencies and Network Types: Between FISMA, FedRAMP, CMMC, SBoM, CFIUS, DoD's APL, and a dozen other procedures and policies, the minimum standards the vendors must comply with can be overwhelming. For industry, they impose barriers to entry. For government, they produce repeated work, complicate information sharing, and drain valuable staff resources. For attackers, they create confusion and inefficiency to exploit. Several coordination efforts can improve the security and efficiency of government acquisition practices, and there are several bodies well-situated to undertake the task—most notably CISA for the federal civilian agency apparatus and the Federal Acquisition Security Council (FASC) across the entire federal government.

- Coordinate and Tier Certifications: Many of the aforementioned processes call back to the same libraries of NIST guidelines, tailoring requirements to agency-, department-, or product-specific needs, but the advantages of common libraries are diminished when processes fail to communicate with each other. For instance, FISMA compliance only maps a vendor to a single agency, and its overlaps with DoD's CMMC requirements, which also draws from a body of NIST controls, do not carry over clearly. Between the various frameworks, there is no common approach to delineation between product, vendor, and acquiring organization, or to tiering the impact level of potential compromise or the security maturity of products or vendors. Agencies should iterate toward a centralized process that still allows custom requirements per agency-specific needs while also reducing repeated work, providing transparency to vendors, and communicating information about remarketed products to different agencies for efficiency.

[244] Shaked Reiner, "Golden SAML: Newly Discovered Attack Technique Forges Authentication to Cloud Apps," CyberArk, November 21, 2017, accessed March 26, 2021, https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps.

- Centralize Information Sharing: Successful *information and communications technology* (ICT) SCRM is ideally a whole-organization endeavor,[245] incorporating input from all stakeholders, including software engineers, intelligence analysts, and chief information officers (CIOs). While internally, agencies are recommended to house ICT SCRM under one body or official, they have largely failed to do so.[246] Among agencies, too, there is not enough communication across different network types, between offense- and defense-oriented entities, and among different auditors. Efforts to centralize communication and risk management within agencies should be replicated within the federal government as a whole, helping to alleviate chronic shortages of expertise and staff resources without sacrificing specialized knowledge of in-house networks.[247]

- Build on Existing, or Potential, Successes: It can be tempting to propose a complete overhaul of the existing, and admittedly chaotic, federal software acquisition and supply chain security regimes. To do so, though, would fail to realize programs that have begun, or are poised to begin, the tasks of improvement. A more efficient approach would draw on those successful instances and generalize their benefits throughout government. For instance, FedRAMP's "do once use many" model can help coordinate among agencies with common needs and vendors with reusable products. The General Services Administration's (GSA's) nascent Polaris program[248] could illustrate methods of lowering cost of entry for smaller firms, and the Vendor Risk Assessment Program (VRAP) included in it can improve information sharing within government, particularly between classified and unclassified intelligence. DoD's CMMC begins the work of tiering security practices and matching them to contract requirements while also requiring basic cyber hygiene of vendors. The FASC is well positioned to centralize ICT SCRM information sharing and acquisition coordination across the whole of government. The National Telecommunications and Information Administration (NTIA) Software Bill of Materials (SBoM) can provide a valuable deliverable metric for a vendor's capacity to track its own dependencies and for agencies to quantify their own risk exposure. CISA's EINSTEIN program could be improved to enhance network monitoring, and its National Cybersecurity Assessment and Technical Services (NCATS) offerings can assess, at

[245] National Institute of Standards and Technology, "*Information and Communications Technology* Supply Chain Risk Management (ICT SCRM)," Department of Commerce, accessed March 26, 2021, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Managements/documents/nist_ict-scrm_fact-sheet.pdf.

[246] Government and Accountability Office, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*.

[247] "Cybersecurity Skills Shortage," McAfee, accessed March 26, 2021, https://www.mcafee.com/enterprise/en-us/about/public-policy/skills-shortage.html.

[248] General Services Administration, "Polaris GWAC Draft Request for Proposals, 47QTCB21N0002," accessed March 26, 2021, https://sam.gov/opp/257509b8cfe14d48beb4f71033995e0b/view.

a technical level, the security of agency networks and vendor practices. The CISA CDM initiative is intended to characterize and track agency assets and infrastructure. Whatever the specific levers of policy, legislation, and bureaucracy that must be pulled, complete overhaul is infeasible—a deliberate analysis of program successes, failures, and potential is necessary to inform sufficient and efficient hardening of the government's software supply chain vulnerabilities. Much like the development process of the software it seeks to secure, rapid and dynamic iteration and improvement of existing programs is needed to realize the potential of disparate government programs.

Conclusion

The security of the software supply chains within the federal government is in dire need of improvement as government relies deeply on acquired software and attacks continue to mount. Fortunately, US President Joseph R. Biden, Jr.'s administration has already indicated[249] cybersecurity, specifically in software supply chains, will be a priority in the coming years, and the new secretary of the Department of Homeland Security is calling[250] for a review of the agency's EINSTEIN and CDM programs, potential points of cross-government coordination. The above lines of improvement outline the weaknesses in the state of federal acquisitions and SCRM practices and indicate broad lines of critical improvement to be pursued.

[249] Eric Geller (@ericgeller), "Neuberger says the Biden admin is developing a new National Cyber Strategy that will incorporate several NSTAC recommendations, including 'promoting software and supply chain assurance' and creating a 'whole-of-nation' approach to emerging technology challenges," Twitter, February 10, 2021, 1:13 p.m., https://twitter.com/ericgeller/status/1359566236934434817.

[250] Justin Katz, "Mayorkas calls for review of EINSTEIN, CDM," FCW, January 19, 2021, accessed March 26, 2021, https://fcw.com/articles/2021/01/19/mayorkas-dhs-confirm-cyber.aspx?m=1.

Appendix C. Advancing a Data Fabric for Achieving Continuous Global Health Protection

Overview

On January 21, 2021, US President Joseph R. Biden, Jr.'s administration released "National Security Directive 1,"[251] a blueprint to advance US leadership on the global stage to "strengthen the international COVID-19 response and to advance global health security and biological preparedness." The directive has several important calls to action, including the rejoining of a number of international health organizations and initiatives, as well as funding important international partnerships and accelerators that focus on therapeutics and vaccine development and distribution. The directive specifically recognizes the intertwined nature of health and wellness for the most vulnerable on the planet, the early detection and deployment of responses to mitigate pathogen and other biological threats, and the security of the United States.

One of the key directives is the establishment of the interagency National Center for Epidemic Forecasting and Outbreak Analytics (NCEFOA) that will help implement "global early warning and trigger systems for scaling action to prevent, detect, respond to, and recover from emerging biological threats." The NCEFOA's forecasting and early warning system echoes the Atlantic Council's call to action for the establishment of a global system for detection, warning, and mitigation. Vaccine and therapeutic development and distribution are identified as key parts of the mitigation response.

Such a bold plan is inherently a data-centric plan, one which will require a responsive network architecture to maintain the key tenets of cybersecurity, interoperability, and the ability to deploy algorithmic intelligence and artificial intelligence (AI) at the edge. This approach proposes an inherently cybersecure network architecture, initially funded by the National Science Foundation (NSF), to solve this problem.

[251] Federation of American Scientists, "National Security Directive on United States Global Leadership to Strengthen the International COVID-19 Response and to Advance Global Health Security and Biological Preparedness," National Security Directive – 1, January 21, 2021, accessed March 26, 2021, https://fas.org/irp/offdocs/biden-nsd/nsd-1.pdf.

Named Data Networking (NDN)[252] is a future Internet architecture whose development was inspired by the recognition of unsolved problems and inherent security risks in the current Internet architecture. One of the fundamental uses of the Internet is to distribute information. The current schema of the Internet is to perform data sharing based on an Internet Protocol (IP) address, or where the data resides. This is *not content secure*, and a number of Band-Aid solutions have been deployed to fix this. These have not proven very effective, as the innumerable hacks of the US healthcare system have demonstrated. These attacks have gone so far as to bring healthcare systems to their knees,[253] infiltrate critical medical supply chains [COVID-19 vaccine cold-chain distribution[254] and personal protective equipment (PPE) procurement[255]], and harvest valuable research and development (R&D) and intellectual property around vaccine development.[256] None of this is compatible with the United States' elevated cybersecurity needs.

NDN, as an Internet architecture, can only be made fully operational with edge devices if a federated identity management system (FIMS) is enabled; this will ensure that data producers at the edge (i.e., humans, healthcare systems, data servers, Internet of Things devices) can be authenticated, and the data they produce wrapped in an individual security wrapper. The data produced is also immutable, version tracked, and cryptographically signed. If such a system were to be hacked, or subject to a ransomware attack, it would not matter, because each piece of content within that container would be protected with these additional layers of security. Further, that data could be logically distributed and stored, and combined only when necessary, e.g., for data aggregation, AI applications, and sense-making. Finally, by securing and addressing data by content, the producers at the edge can become data owners. That means, citizens or municipalities whose healthcare data are interacting with the system at the edge can own encrypted versions of their personal data that are similarly difficult to hack, and then transact with it. In the process of securing the data with this alternate

[252] "Named Data Networking: Motivation & Details," Named Data Networking, accessed March 26, 2021, https://named-data.net/project/archoverview/; "NDN Community Meeting, September 10-11, 2020," NIST, accessed March 26, 2021, https://www.nist.gov/news-events/events/2020/09/ndn-community-meeting; Cameron Ogle et al., "Named Data Networking for Genomics Data Management and Integrated Workflows," Frontiers in Big Data, February 15, accessed March 26, 2021, https://www.frontiersin.org/articles/10.3389/fdata.2021.582468/full.

[253] Jessica Davis, "UPDATE: The 10 Biggest Healthcare Data Breaches of 2020, So Far," HealthITSecurity, July 8, 2020, accessed March 26, 2021, https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020-so-far.

[254] Cybersecurity and Infrastructure Security Agency, "IBM Releases Report on Cyber Actors Targeting the COVID-19 Vaccine Supply Chain," original release date: December 03, 2020, accessed March 26, 2021, https://us-cert.cisa.gov/ncas/current-activity/2020/12/03/ibm-releases-report-cyber-actors-targeting-covid-19-vaccine-supply.

[255] Rich Haridy, "COVID-19 vaccine distribution networks targeted by hackers," New Atlas, December 3, 2020, accessed March 26, 2021, https://newatlas.com/computers/hackers-target-covid-19-vaccine-distribution-networks/.

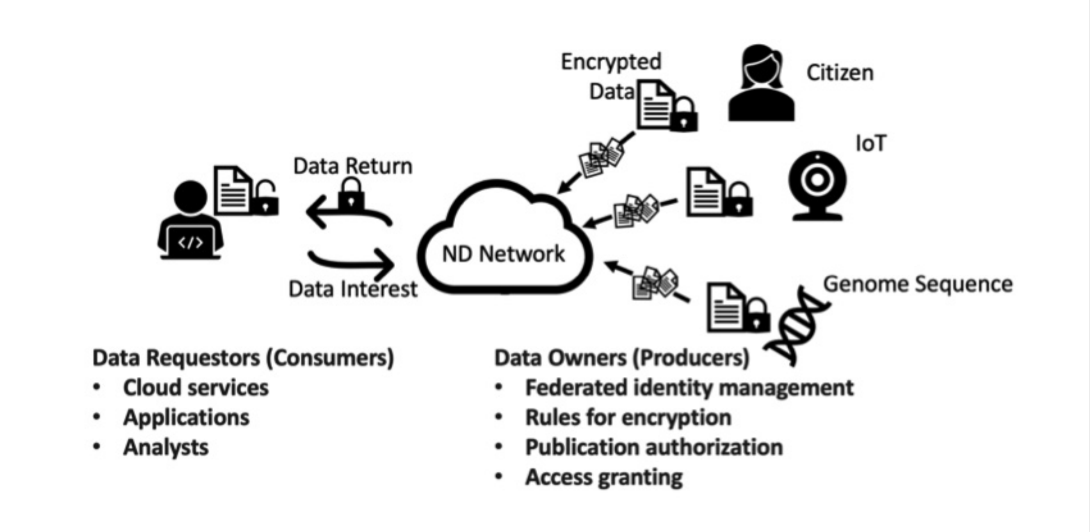
[256] James Purtill, "Cozy Bears and Hidden Cobras: The hackers targeting COVID-19 vaccine researchers," ABC Science, December 14, 2020, accessed March 26, 2021, https://www.abc.net.au/news/science/2020-12-15/covid-19-coronavirus-the-hackers-targeting-vaccine-researchers/12974504.

Internet architecture, a mechanism for establishing data trusts and only sharing necessary data is enabled. This model of data ownership further enables a type of fiduciary trust in which even public–private partnerships (PPPs) will not result in private interests capturing data for commercial or shareholder interests.

Thus, a content-based Internet data fabric with edge device security and authentication provides these value propositions:

- Establishment of a "total trust network" comprising independently owned and authorized private vaults that share a common security and information framework;
- Trusted user, device, and application identity, e.g., human, computer, IoT, sensors;
- Data owner/producer-controlled data sharing and exposure based primarily on the entity and/or transaction—the who, what, when, and how;
- Fully protected data exchange, verification, and immutability between authorized entities available anywhere and anytime, without the threat of data leaks, ransomware, or hacking;
- Easy integration into existing networks;
- Deployment on any private or public cloud architecture; and
- Support for all existing supplementary authentication methodologies (e.g., multifactor).

Figure C.1: Schematic for Secure Network with Data Producers and Consumers

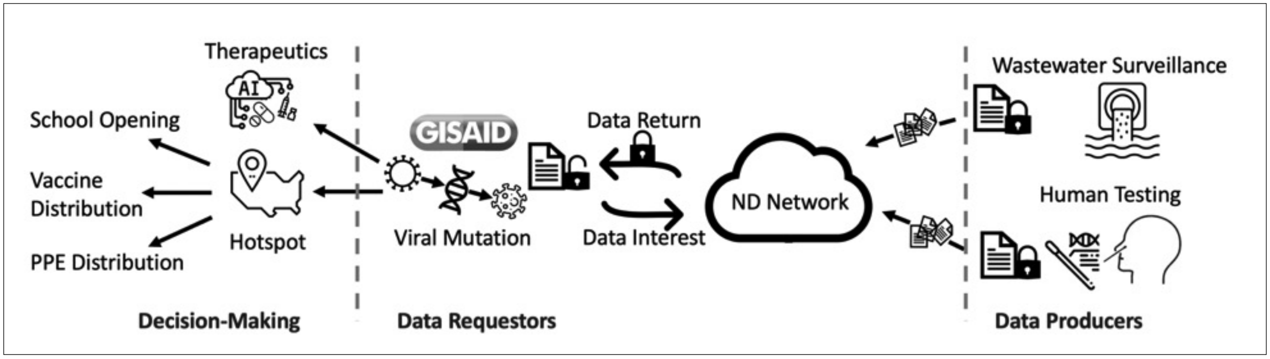


This work proposes two testbed models for this future Internet architecture to secure the United States' critical healthcare data and infrastructure.

Model 1: Testbed for the National Center for Epidemic Forecasting and Outbreak Analytics (NCEFOA) to prevent, detect, respond to, and recover from emerging biological threats.

The first model is a wastewater surveillance and pathogen sequencing/mutation network, in which municipal wastewater surveillance can be combined with individual viral testing and sequencing. Such data might be requested by federal, state, and local health agencies to identify hot spots early and track viral mutations by locale. It would also enable the detection of novel pathogens by sequence. This information may then be used to direct the development of AI-based therapeutics and critical policy and economic decision making, such as driving alert systems, directing school and business openings, and identifying vulnerable zip codes for rapid vaccine/therapeutics distribution, as well as healthcare resource distribution such as PPE, medical personnel, beds and ventilators.

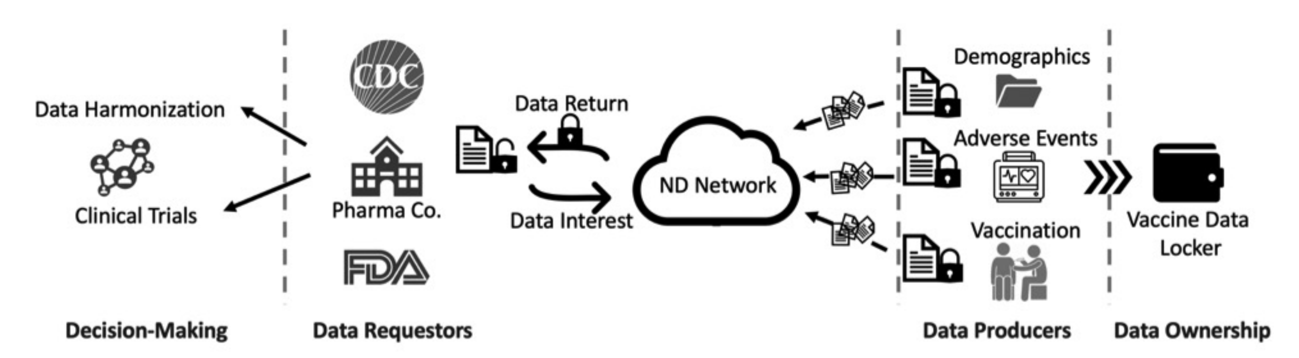
Figure C.2: Wastewater Surveillance and Viral Mutation Integration Network



Model 2: Testbed for a response to coordinate vaccine and therapeutic development and distribution.

The second model is a vaccine distribution application based on the enhanced cybersecurity provided by the NDN. This application would enable both the tracking of vaccine (lot, dose, timing) and recipient demographics (source encryption). It would further enable data harmonization and a system for reporting adverse viral events to health officials, the Centers for Disease Control and Prevention (CDC), the Food and Drug Administration (FDA), and to pharma companies, so they can continue to perform Phases III and IV clinical trials in the pursuit of FDA clearance and human safety. The vaccine tracking system would also enable tracking of surplus vaccine for eventual donation to global vaccine pools. Early deployment would be compatible with the Federal Emergency Management Agency (FEMA)-based vaccination centers announced by the Biden administration. Alternatively, the application could be deployed on the vaccine provider side to assist with the distribution of vaccines in underserved areas within the United States (e.g., rural areas, Navajo Nation).

Figure C.3: Vaccine Distribution Network Application with Vaccine Data Lockers



A key element is an advanced polymorphic trust network architecture that is decentralized, reliable, resilient, and cybersecure to enable the administration to reach key goals within "National Security Directive-1." The trust network architecture is virtually impervious to hacking and ransomware attacks because the data are immutable and signed. In addition, there are two model testbeds that answer needs within the directive—one for early detection and warning, by combining wastewater surveillance, pathogen testing, and mutation analysis; and the second for vaccine distribution, adverse events reporting, and data ownership, that would also enable pharma to conduct ongoing, secured, digital clinical trials. The system also provides for implementing a public data trust, within a decentralized system, in which much of the fiduciary responsibility for the data lies in the naming and immediate securing of sensitive, immutable data as it is generated, and identity management and authentication of key stakeholders. This permits data sharing only between authenticated producers and receivers, and removes the data profit or surveillance motive in gathering data for critical intelligence. Often these types of data gathering do not reconcile well with the cornerstones of democracy, such as public ownership and participation. The network architecture is compatible with the seemingly opposing directives of intelligent surveillance and civil liberties.

This framework delivers a virtually impenetrable mechanism with a higher degree of trust that is essential to securing our cyberhealth and R&D, and digitally transacting with sensitive biometric data. It will enable the United States to move forward with data-centric policies that both enable edge data intelligence and integration of new and existing networks involved in sensing capabilities, while protecting Americans' civil liberties. Furthermore, it provides a new, secure network architecture that can integrate the vast number of sensors and bidirectional IoT devices coming online. In addition to securing the United States' cyberhealth infrastructure, the network architecture plus federated identity management and authentication would be valuable for securing infrastructure, communications, sensor data, voting data, and enabling things like digital identities, commerce, and banking.

Appendix D. Additional Readings on the History and Future of Global Space Governance

By 2050, numerous studies indicate that the commercial space industry will reach a valuation of more than $3 trillion. In response, there has been much interest among policy makers in the potential geopolitical, economic, and social ramifications that will result from this expansion. In their attempts to quickly tap into this market, however, there has been one area that has yet to receive much scrutiny: the space governance regime itself. As more private industries expand into this domain, they are likely to run into an outdated governance regime that has seen little modification since the Cold War. Drafted and codified in an era when space was dominated by two major nation-states, these regulations have yet to be framed to reflect a new era of space commercialization and management. Unaddressed, inflexibilities in the current regime could hinder the successful development of outer space, creating a range of problems for both the private and public sectors. While broad solutions have yet to be found, any well-informed debate on the future of space must include discussions on the challenges of governing space, issues that have vexed policy makers since the 1950s. For the GeoTech Decade, leaders from all sectors, nations, and industries must be aware of the hazards and potential solutions ahead. Listing from chronological order from 2015 to 2021, plus one entry from 2011, the following readings represent scholarly research on this evolving topic area.

1. Toward a Theory of Space Power: Selected Essays

Editors: Charles D. Lutes, Peter L. Hays, Vincent A. Manzo, Lisa M. Yambrick, and M. Elaine Bunn

Publication date: 2011

Publisher: National Defense University Press, Washington, D.C.

Excerpts from the publication:

> Chapter 3: International Relations Theory and Space Power (Robert L. Pflatzgraff Jr.)
>
> “Because the stakes are immense, how we theorize about space, drawing on existing and yet-to-be-developed IR and other social science theories, will have major implications for strategies and policies. Because no single IR theory capable of describing, explaining, or prescribing political behavior on Earth exists, we cannot expect to find otherwise in space. Therefore, it is important to recognize the inherent limitations in extrapolating from Earthly IR theory to space, while also drawing wherever possible on such theory as we probe farther into space. “
>
> Chapter 11: Merchant and Guardian Challenges in the Exercise of Space Power (Scott Pace)
>
> “[T]he Outer Space Treaty, by barring claims of sovereignty, is usually thought to bar private property claims. Many legal scholars in the International Institute of Space Law and other organizations support that view. Other scholars, however, make a distinction between sovereignty and property and point to civil law that recognizes property rights independent of sovereignty. It has also been argued that while Article II of the treaty prohibits territorial sovereignty, it does not prohibit private appropriation. The provision of the Outer Space Treaty requiring state parties to be responsible for the activities of persons under their jurisdiction or control leaves the door open to agreements or processes that allow them to recognize and confer property rights, even under common law.
>
> “Current international space treaties are built on the assumption that all matters can and should trace back to states. This is in contrast to admiralty law and the growing field of commercial arbitration in which the interests and responsibilities of owners, not necessarily the state, were the legal foundation. It can be argued that the Outer Space Treaty was not the final word on real property rights in space even within the international space law community, as drafters of the 1979 Moon Treaty felt it necessary to be more explicit on this point.
>
> “Legal issues will become increasingly more important as the ‘Vision for Space Exploration’ proceeds and humans attempt to expand farther and more permanently into space. In exercising spacepower, the United States should seek to ensure that its citizens have at least as many rights and protections in space, including the right to own property, as they do on Earth. Whether such rights would be as complete as those in the United States would be the subject of negotiation and debate. Simply put, however, the Moon and other celestial bodies should not be a place of fewer liberties than those enjoyed on Earth.”

Link: https://ndupress.ndu.edu/Portals/68/Documents/Books/spacepower.pdf

2. 'How Simple Terms Mislead Us: The Pitfalls of Thinking About Outer Space as a Commons'

Authors: Henry R. Hertzfeld, Brian Weeden, and Christopher D. Johnson

Publication date: 2015

Publisher: Secure World Foundation

Excerpt from the publication:

> "Thinking about space as a global commons may be a laudatory ideal, and one that perhaps can be regarded as a very long-term goal for society. But it is hardly a practical solution or goal for the problems we face today, witnessed by at least a thousand years of precedent in law and practice coupled with radically different technologies, exponential world population growth from 500 million people (at most) in Roman times and the Middle Ages to over 7 billion people today, and other radical political and social changes.
>
> "But all of the ways we try to phrase 'benefits to all mankind,' 'province of all mankind,' etc. have their limits. Treaty guarantees such as no sovereignty are not the same as limiting ownership, property rights, and establishing the concept of national liability for activities and human behavior in space.
>
> "Attempts to develop some sort of overall 'governance' of space based on a res communis principle will not succeed in today's political environment. (Or, quite likely in any form where nations have the ability to interpret treaty language differently and where different forms of government exist.)"

Link: https://swfound.org/media/205390/how-simple-terms-mislead-us-hertzfeld-johnson-weeden-iac-2015.pdf

3. National Security Space Defense and Protection

Publication Date: 2016

Publisher: The National Academies Press

Excerpt from the publication:

> "The significant difference, of course, between the creation of global maritime policy and practice and that of the space domain is time. The technologies, customary behaviors, conventions and, eventually, treaties governing military and commercial naval activity evolved over centuries along with the enabling operational concepts, naval strategies, nation-states and attendant diplomacy. The system was thus able to gradually incorporate advances, slowly accommodate stresses, and, to some degree, resolve conflicts in a deliberate manner over time.
>
> "A key aspect of space is that the speed of advances in access and spaceborne capabilities has significantly outpaced the creation of guiding national-let alone international strategies and policies. The technological advances in space

> systems and increased reliance on them have created a space-enabled 'critical infrastructure' that has not been matched by coherent supporting protection and loss-mitigation strategies, clearly articulated and accepted policies, and robust defensive capabilities. These gaps have created newfound concern domestically, confusion on the part of allies, and opportunities for misalignment and misperceptions on the part of potential adversaries. The need to rapidly, precisely, and effectively address all of these factors has created an environment of urgency to find mitigation strategies, fill policy gaps, and fund new capabilities. Done poorly, rapid efforts and expansive rhetoric can exacerbate existing tensions, pursue capabilities that add only marginally to system security, and increase the probability of misunderstanding or miscalculation on the part of potential adversaries. Well coordinated and properly executed, these efforts can meet real needs, add essential system security, and promote stability. These efforts must succeed. National security and global stability in space and on Earth demand it."

Link: https://doi.org/10.17226/23594

4. 'Space Development, Laws, and Values'

Author: Scott Pace, executive secretary, National Space Council

Date: December 13, 2017

Details: Speech to the IISL Galloway Space Law Symposium, Cosmos Club, Washington, DC

Excerpt from the speech:

> "[I]n today's world, technology and entrepreneurship threaten to outpace the legal and domestic regulatory mechanisms intended to enable and manage space activities. When technological generations occur every 18 months or so, it would appear to outside observers that the pace of international space discussions at the United Nations is, by comparison, glacial. As many of you know, the development of voluntary 'best practices' for the long-term sustainability (LTS) of outer space activities at the UN Committee on the Peaceful Uses of Outer Space is expected to be finalized next year after years of cooperative, but sometimes contentious, efforts. In the intervening time since LTS discussions began, we have seen many new developments, from new space start-ups, reusable rockets, and proposals for mega-constellations, alongside more traditional governmental space activities.
>
> "U.S. leadership requires active engagement in interpreting and implementing existing space agreements and other international law, while pursuing non-binding 'best practices' and confidence-building measures with our allies, security partners, and potential adversaries to meet today's space challenges. It necessitates enacting transparent, effective, and minimally burdensome domestic legislation and regulatory mechanisms to enable U.S. companies to benefit from technology development and new commercial opportunities."

Link: https://spacepolicyonline.com/wp-content/uploads/2017/12/Scott-Pace-to-Galloway-FINAL.pdf

5. Handbook for New Actors in Space

Editor: Christopher D. Johnson

Publication date: 2017

Publisher: Secure World Foundation

Excerpt from passage:

> "Space is changing. The barriers to access to space are decreasing. Shrinking costs, less infrastructure, and lower technological hurdles all make space activities available to more people. Meanwhile, smaller programs with fewer necessary personnel enable more states and entities to participate in space projects. Nevertheless, regardless of a space project's size, the existing international legal and regulatory framework underpins and permits space activities. This regime is decades old and was created in a different geopolitical context. Some feel it is ill-suited for the next half-century of space activities—either too restrictive, or not sufficiently clear in its requirements."

Link: https://commons.erau.edu/cgi/viewcontent.cgi?article=1006&context=db-cso-351-spring2019

6. 'Space, the Final Economic Frontier'

Author: Matthew Weinzierl

Publication date: 2018

Publisher: *Journal of Economic Perspectives*, Volume 32, Number 2, Pages 173-192

Excerpt from the publication:

> "The vulnerabilities of centralized control will be familiar to any economist: weak incentives for the efficient allocation of resources, poor aggregation of dispersed information, and resistance to innovation due to reduced competition. In addition to these concerns, NASA's funding and priorities were subject to frequent, at times dramatic, revision by policymakers, making it hard for the space sector to achieve even the objectives set at the center (Handberg 1995; Logsdon 2011).
>
> "Anticipating these vulnerabilities, reform advocates had made previous pushes for at least partial decentralization and a greater role for the private sector in space. Near the dawn of the Shuttle era, President Ronald Reagan signed the Commercial Space Launch Act of 1984, saying: 'One of the important objectives of my administration has been, and will continue to be, the encouragement of the private sector in commercial space endeavors.' That same year saw the creation of the Office of Commercial Programs at NASA and the Office of

> Commercial Space Transportation in the Department of Transportation (NASA 2014). However, these early seeds would have to wait until the end of the Shuttle program to bear fruit."

Link: https://www.hbs.edu/ris/Publication%20Files/jep.32.2.173_Space,%20the%20Final%20Economic%20Frontier_413bf24d-42e6-4cea-8cc5-a0d2f6fc6a70.pdf

7. 'Space Technology and the Implementation of the 2030 Agenda'

Author: Simonetta DiPippo

Publication date: 2019

Publisher: *UN Chronicle*, Volume 55, Issue 4, Pages 61-63

Excerpt from the publication:

> "There are already many tangible changes and challenges to the traditional ways of conducting space activities, with many new actors entering the field and new technologies affecting our efforts. When the space age began with the launch of Sputnik 1 in 1957, only two countries were active in the space environment. Today, we have over 70 national and regional space agencies working to extend our knowledge of space and apply space science and technology to improve the lives of people worldwide. Thousands of other actors are also joining the space community, with a well-established private space sector.
>
> "With the rapid expansion of stakeholders accessing space, the estimated value of the space sector reached an all-time high of $383.5 billion in 2017, with commercial space activities accounting for over 75 per cent of that value. Such statistics demonstrate the extent to which private entities have become major players in the field. Projections for the future value of the sector show it rising at an exponential pace, reaching $1.1 trillion to $2.7 trillion over the next 30 years."

Link: https://www.un.org/en/chronicle/article/space-technology-and-implementation-2030-agenda

8. ‘Catalyzing Space Debris Removal, Salvage, and Use’

Authors: Peter Garretson, Alfred B. Anzaldúa, and Hoyt Davidson

Publication date: 2019

Publisher: *The Space Review*

Excerpt from the publication:

> “[S]alvage and debris cleanup is very difficult under the current international legal space regime and orbital conditions, all of which disincentivize action. First, per Article VIII of the Outer Space Treaty (OST), a State Party on whose registry an object is launched into outer space retains jurisdiction and control of the items launched. Moreover, Articles VI and VII of the OST and Article IV of the Liability Convention make multiple launching states involved in a space debris intervention jointly and severally liable for any harm or damage to the persons or property of other States Parties.
>
> “Further complicating liability assessment, a lot of orbital debris is unclaimed and neither the spacecraft owner nor operator nor the launching state can be determined. According to Brian Weeden of the Secure World Foundation, ‘Of the 500,000 estimated human-generated objects in orbit bigger than one centimeter, we only know which country put it there for about 16,000 objects. And less than half of those 16,000 were registered with the UN.’ Moreover, deorbiting debris will often require moving the junk through lower orbits. Further aggravating the issue, moving debris to salvage yards for later use will sometimes require moving the debris through higher orbits. In each case, there will likely be an increased risk of collision or other accidents.
>
> “While it may be unclear if anyone is liable for unclaimed debris, it can be argued that the moment a State Party to the OST, via its national entity, touches the debris, the State Party assumes liability for whatever happens according to Article VI of the OST, which mandates that State Parties bear ‘international responsibility’ for national activities in outer space and also requires ‘authorization and continuing supervision’ of the involved national actors.”

Link: https://www.thespacereview.com/article/3847/1

9. War in Space: Strategy, Spacepower, Geopolitics

Author: Bleddyn E. Bowen

Publication date: 2020

Publisher: Edinburgh Press

Excerpt from the publication:

> "Today, over 2,000 active satellites are deployed in Earth orbit by over seventy states and commercial entities. The global space economy in 2018 was worth around US$360 billion. The uses of satellites and the potential consequences of their denial in a time of war are generating strategic effects that strategists and scholars must account for. The infrastructural and support services derived from orbital satellite constellations remains an under-theorised and under-conceptualised techno-geographic phenomenon in IR and strategic studies. These satellites provide a range of functions for military, economic, civilian, intelligence and scientific needs.
>
> "The proliferation of those technologies outside the United States is eroding one of the main advantages Western militaries have enjoyed since the end of the Cold War, levelling somewhat the conventional military and economic balances of the 'great powers' with significant implications for global power relations in the twenty-first century. Earth's major powers are exploiting their own space infrastructure and pursuing space weapons technology which have undermined an oft-assumed American dominance of outer space, but it has not necessarily ended American power preponderance on Earth"

Link: https://marketplace.officialstatistics.org/privacy-preserving-techniques-handbook

10. 'Executive Order 13914 of April 6, 2020: Encouraging International Support for the Recovery and Use of Space Resources'

Author: United States Government

Publication date: April 6, 2020

Publisher: Executive Office of the President, United States Government

Excerpt from the Executive Order:

> "Successful long-term exploration and scientific discovery of the Moon, Mars, and other celestial bodies will require partnership with commercial entities to recover and use resources, including water and certain minerals, in outer space.
>
> "Uncertainty regarding the right to recover and use space resources, including the extension of the right to commercial recovery and use of lunar resources, however, has discouraged some commercial entities from participating in this enterprise. Questions as to whether the 1979 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (the 'Moon Agreement') establishes the legal framework for nation states concerning the recovery and use of space resources have deepened this uncertainty, particularly because the United States has neither signed nor ratified the Moon Agreement. In fact, only 18 countries have ratified the Moon Agreement, including just 17 of the 95 Member States of the United Nations Committee on the Peaceful Uses of Outer Space.

> Moreover, differences between the Moon Agreement and the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies—which the United States and 108 other countries have joined—also contribute to uncertainty regarding the right to recover and use space resources."

Link: https://www.federalregister.gov/documents/2020/04/10/2020-07800/encouraging-international-support-for-the-recovery-and-use-of-space-resources

11. 'Space Governance in the New Space Era'

Authors: Daniel L. Oltrogge and Ian A. Christensen

Publication date: 2020

Publisher: *Journal of Space Safety Engineering*, Volume 7, Issue 3, Pages 432-438

Excerpt from the publication:

> "Applied to space activities, adaptive governance is the idea that 'you can't effectively regulate what you don't know' (e.g., technological approaches, business models); yet for new applications, regulations are needed to provide legal certainty and common rules and to satisfy international obligations. Achieving this balance requires a system of regular updates to regulatory provisions and frameworks, rather than attempts to address new applications in totality. It also requires exchanges of information between technical, economic, business, policy and regulatory communities. It is a philosophy of governance, rather that specific structure or approach. For example, an international working group developing a set of legal building blocks to enable commercial utilization of space resources has found that it is 'neither necessary nor feasible to attempt to comprehensively address space resource activities in the building blocks: space resource activities should be incrementally addressed at the appropriate time on the basis of contemporary technology and practices"

Link: https://www.sciencedirect.com/science/article/pii/S2468896720300550?via%3Dihub

12. 'The US National Space Policy (2020)'

Authors: United States Government

Publication date: 2020

Publisher: Executive Office of the President, United States Government

Excerpt from the publication:

> "It is the policy of the United States to ensure that space operations are consistent with the following principles.

(1) It is the shared interest of all nations to act responsibly in space to ensure the safety, stability, security, and long-term sustainability of space activities. Responsible space actors operate with openness, transparency, and predictability to maintain the benefits of space for all humanity.

(2) A robust, innovative, and competitive commercial space sector is the source of continued progress and sustained United States leadership in space. The United States remains committed to encouraging and facilitating the continued growth of a domestic commercial space sector that is globally competitive, supports national interests, and advances United States leadership in the generation of new markets and innovation-driven entrepreneurship.

(3) In this resurgent era of space exploration, the United States will expand its leadership alongside nations that share its democratic values, respect for human rights, and economic freedom. Those values will extend with us to all space destinations as the United States once again steps beyond Earth, starting with the Moon and continuing to Mars.

(4) As established in international law, outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means. The United States will pursue the extraction and utilization of space resources in compliance with applicable law, recognizing those resources as critical for sustainable exploration, scientific discovery, and commercial operations.

(5) All nations have the right to explore and to use space for peaceful purposes and for the benefit of all humanity, in accordance with applicable law. Consistent with that principle, the United States will continue to use space for national security activities, including for the exercise of the inherent right of self-defense. Unfettered access and freedom to operate in space is a vital national interest.

(6) The United States considers the space systems of all nations to have the right to pass through and conduct operations in space without interference. Purposeful interference with space systems, including supporting infrastructure, will be considered an infringement of a nation’s rights. Consistent with the defense of those rights, the United States will seek to deter, counter, and defeat threats in the space domain that are hostile to the national interests of the United States and its allies. Any purposeful interference with or an attack upon the space systems of the United States or its allies that directly affects national rights will be met with a deliberate response at a time, place, manner, and domain of our choosing.”

Link: https://www.federalregister.gov/documents/2020/12/16/2020-27892/the-national-space-policy

13. Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity

Authors: Bruce McClintock, Katie Feistel, Douglas C. Ligor, and Kathryn O'Connor

Publication date: 2021

Publisher: RAND Corporation

Excerpt from the publication:

> "In the early days of space exploration, few actors had the resources and motivation to place satellites on orbit. Therefore, there was less concern over space traffic, and the focus was primarily on tracking satellites with basic position information to send and receive information or commands. As space has become more congested, the importance of safety from collisions has increased in importance. Safety in space hinges on the ability to carry out a satellite's mission without unintentional interference. The growing number of space actors, space objects, and space debris in the New Space Era creates challenges for operating safely in space. To provide a sense of magnitude, some estimate that 96 percent of space objects are untracked and the number of satellites on orbit could increase by four to ten times in the next decade. Maintaining a safe environment in space requires a chain of interconnected activities that includes detection, tracking, communication and coordination between users, and, if necessary, commands to maneuver satellites to prevent potential collisions. There is also the need for more debris management to mitigate the ever-increasing buildup of inactive objects in space. Nearly every step in this chain has shortcomings, so there is a compelling need to improve overall safety activities."

Link: https://www.rand.org/pubs/perspectives/PEA887-2.html

14. The Outer Space Treaty: Overcoming Space Security Governance Challenges

Author: Rajeswari Pillai Rajagopalan

Publication date: 2021

Publisher: Council on Foreign Relations

Excerpt from the publication:

> “These trends are proving to be a growing challenge for existing global governance mechanisms. Outer space activities are governed by a number of treaties and agreements, the foundation of which is the 1967 Outer Space Treaty (OST)—or, more formally, the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies. But these agreements were developed in the 1960s and 1970s, and they are showing their age. Constructed under different geopolitical and technological circumstances, they are not well-suited for addressing contemporary challenges.
>
> “Legally binding measures, including revising the OST, should be pursued in earnest, but the political impediments to developing new measures or amending existing measures are challenging to overcome. Given that the difficulties arise mostly from political disagreements, nonlegal, political instruments such as transparency and confidence-building measures (TCBMs) should also be pursued. While legal measures such as reforming the OST still need to be considered the end goal, this working paper recommends a step-by-step approach to addressing the political difficulties of developing effective rules of the road.
>
> “Two opposing perspectives prevail on global governance in outer space—one that believes that legal measures are necessary to resolve the problems facing the current space regime and another that argues that, given the contemporary political climate, traditional TCBMs are the more practical goal.”

Link: https://www.cfr.org/report/outer-space-treaty

Appendix E. Informational GeoTech Center Synopses

1. 5G's Geopolitics Solvable by Improving Routing Protocols against Modern Threats[257]

Author: David Bray, PhD

April 9, 2020

The article is accessible at:

https://www.atlanticcouncil.org/blogs/geotech-cues/5gs-geopolitics-solvable-by-improving-routing-protocols-vs-modern-threats

This article addresses the fear, uncertainty, and doubt that have been cast on the 5th Generation of International Mobile Telecommunications standards (5G), which has become a geopolitical point of contention between China and the United States. 5G standards themselves still have to be finalized internationally, making it even more difficult to discern market reality versus market positioning versus market hype.

As such, having performed a deeper dive into the issues surrounding 5G over the last few months, the GeoTech Center proposes to global policy makers that the geopolitical tensions associated with 5G, as well as other geopolitical cybersecurity-related concerns, can be solved by improving routing protocols against modern threats. Such an endeavor would require a commitment from multiple parties to advance the state-of-the-art in content- and trust-based routing protocols in terms of research and development, with an eye to future benefits in three to five years.

The purpose of this article is to motivate global policy makers and industry leaders to develop and demonstrate a governance protocol by which an individual communications network device can evolve one or more trustworthy communication pathways in a heterogeneous communications environment amid potentially deceptive and disruptive nodes.

Key conclusions include the following:

[257] David Bray, "5G's geopolitics solvable by improving routing protocols against modern threats," Atlantic Council, April 9, 2020, accessed March 26, 2021, https://www.atlanticcouncil.org/blogs/geotech-cues/5gs-geopolitics-solvable-by-improving-routing-protocols-vs-modern-threats/.

- If consumers or markets are concerned that 5G technologies are being used surreptitiously for intelligence purposes without their consent, that will erode trust in open societies and free markets.
- Internet-based routing includes the Border Gateway Protocol (BGP). Unfortunately, BGP lacks cryptographic identification that can prove Autonomous Systems (ASes) providing routing information are who they claim or that the information they provide on behalf of other ASes can be trusted. To fix this, Secure BGP and related approaches attempt to overcome the vulnerabilities present in BGP, yet so far Secure BGP and similar efforts to address these vulnerabilities have proven economically difficult to deploy at scale. Even then, like BGP, Secure BGP itself has limits on the growth of the routing table.
- 256 GB of NAND flash memory simply has not been available for most of the history of the Internet and mobile communications; now it is available cheaply and will continue getting cheaper as data centers are driving this decrease in cost. NAND stores data in arrays of memory cells that are made using floating-gate transistors.
- At the same time, 5G should reduce latency and increase bandwidth. As a result, sending out exploratory packages is now possible for densely connected workers in ways that were not possible with 2G or 3G. Also, onboard computing is able to do more than what was possible in the past; a palm-size device now does twenty teraflops using x86 architectures at low energy/via solar power.
- Regardless of 5G, 4G, or any other mobile telecommunications standards, the era in which on-system memory limits prevented storing the necessary information about potential nodes from which to evolve trust is over.

2. Space Salon: Making Space Available to Everyone[258]

Panelists: Joseph Bonivel, Jr., nonresident senior fellow at the Atlantic Council's GeoTech Center; Paul Jurasin, director of New Programs/Digital Transformation Hub at Cal Poly State University; Jody Medich, principal design researcher, Microsoft Office of the CTO; Michael Nicolls, principal engineer at SpaceX and founding CTO of LeoLabs, Inc.; and Simon Reid, chief operating officer, D-Orbit UK.

July 8, 2020

The recording is accessible at the following link:

[258] Atlantic Council, "Space salon: Making space available for everyone," July 8, 2020, accessed March 26, 2021, https://www.atlanticcouncil.org/event/space-salon-making-space-available-for-everyone/.

https://www.atlanticcouncil.org/event/space-salon-making-space-available-for-everyone/

In this event, panelists discuss how space operations are transitioning from an industry heavily driven by government funding and strategy to a commercially focused and self-sufficient market. The private sector now regularly invests in rockets, satellite hardware, and experiments in space to advance its business interests, driving a shift in how the space industry operates and thrives. As the National Aeronautics and Space Administration (NASA) and other space agencies gradually transition responsibility for orbital safety activities to the commercial world, private companies will increasingly assume the risks of space travel and operations in space.

The event concluded that:

- The current period marks the beginning of space commercialization. Innovation as well as novel applications of existing technology, such as using virtual reality (VR) to accelerate training for space operators, will continue to lower barriers to entry. Nevertheless, both commercial and government actors can take actionable steps to make space available for everyone.
- There remain significant barriers to entry in the commercial space sector. Of course, the physical requirements to launch a satellite into low-Earth orbit are substantial, intensified by multiplying debris in space. Government regulatory hurdles further dissuade firms from potentially entering the commercial space sector. Future efforts must be aimed at reforming regulation to encourage competition and innovation.
- A lack of data standardization may hinder innovation in space. Private companies gather massive amounts of satellite data which largely remains siloed on company servers. Industry must develop its own open-source data standards to foster collaboration. Governments should step in later, recognizing that industry moves faster. Once standards are developed, firms should move toward building networks of satellites with integrated sensors and automated collision avoidance systems.
- Governments must facilitate innovation, promote transparency, and ensure equitable access to space. Updating regulatory frameworks to encourage responsible private sector coordination represents a promising first step. Governments should also begin sharing more data to promote transparency. Lastly, governments need to adopt policies on space commercialization that benefit everyone: a rural farmer should have just as much access to data collected in space as a multinational corporation.

3. Building a Collaborative Ecosystem for AI in Healthcare in Low- and Middle-Income Economies[259]

Authors: Abhinav Verma, Krisstina Rao, Vivek Eluri, and Yukti Sharma

August 27, 2020

The article is accessible at:
https://www.atlanticcouncil.org/content-series/smart-partnerships/building-a-collaborative-ecosystem-for-ai-in-healthcare-in-low-and-middle-income-economies/

In this article, the Atlantic Council's GeoTech Center discusses how over the past two decades AI has emerged as one of the most fundamental and widely adopted technologies of the Industrial Revolution 4.0. AI is poised to generate transformative and disruptive advances in healthcare through its unparalleled ability to translate large amounts of data into actionable insights for improving detection, diagnosis, and treatment of diseases; enhancing surveillance and accelerating public health responses; and now, for rapid drug discovery as well as interpretation of medical scans.

Given its range of applications, AI will undoubtedly play a central role in most nations' journeys toward Universal Health Coverage (UHC) and the United Nations Sustainable Development Goals (SDGs).[260] However, the development of AI for healthcare has been largely disparate[261] in low- and middle-income countries (LMICs) relative to high-income countries (HICs) even as their public health conditions are converging. As incomes have grown across the developing world, health outcomes and life expectancies in LMICs have markedly improved,[262] growing closer to those in HICs. This development has ignited a growing demand for services, rising costs of delivery and innovation, and challenges in building the appropriate workforce to deliver care.[263]

[259] Abhinav Verma et al., "Building a collaborative ecosystem for AI in healthcare in Low and Middle Income Economies," Atlantic Council, August 27, 2020, accessed March 26, 2021, https://www.atlanticcouncil.org/content-series/smart-partnerships/building-a-collaborative-ecosystem-for-ai-in-healthcare-in-low-and-middle-income-economies/.

[260] United Nations, *Report of the Secretary-General on SDG Progress 2019, Special Edition*, accessed March 26, 2021, https://sustainabledevelopment.un.org/content/documents/24978Report_of_the_SG_on_SDG_Progress_2019.pdf.

[261] Ahmed Hosny and Hugo J.W.L. Aerts, "Artificial intelligence for global health," Science, 366 (6468) (November 22, 2019): 955–956, DOI: 10.1126/science.aay5189, accessed March 26, 2021, https://science.sciencemag.org/content/366/6468/955/tab-figures-data

[262] Esteban Ortiz-Ospina and Max Roser, "Global Health," Our World in Data, 2016, https://ourworldindata.org/health-meta.

[263] McKinsey & Company, *Transforming healthcare with AI, The impact on the workforce and organisations*, March 2020, accessed March 26, 2021, https://eithealth.eu/wp-content/uploads/2020/03/EIT-Health-and-McKinsey_Transforming-Healthcare-with-AI.pdf.

This article concludes that:

- There is a large disparity in health outcomes in LMICs and HICs despite their having similar health conditions and incidents. This is evident in maternal mortality, under-five mortality, and instances of communicable disease. Many AI initiatives have been implemented to close this gap. AI is expected to help in the areas of access, safety, quality of care, efficiency, and education.
- These emerging transformations of healthcare technologies are most needed in LMICs. However, AI experimentation comes with complications because to support these initiatives it is imperative that a country has data availability, business model sustainability, and strong infrastructure, elements that may be in short supply in an LMIC. To counter this, the World Health Organization (WHO) produced a strategic plan for countries to prepare themselves for supporting eHealth systems. That plan includes policies, legislation, and standards.
- The best way to implement a functioning AI program is to start with data collection and management, and data sharing. Data privacy is a top concern in LMIC governments and stakeholders. As a result, it is recommended that regulations mandate and record all data to a set of standards. Open-source data banks, annotation tools, designated collaborative platforms, and peer reviews are the best way to achieve this.

4. Western Society at the Crossroads, Part II: Smart Partnerships in a Changing World[264]

Panelists: Mathew Burrows, director of the Atlantic Council's Foresight, Strategy, and Risks Initiative; Asha Jadeja Motwani, Founder, Motwani Jadeja Foundation; Julian Mueller-Kaler, resident fellow at the Atlantic Council's GeoTech Center and senior fellow at the Foresight, Strategy, and Risks Initiative; and Michael Schaefer, Chairman of the Board of Directors, BMW Foundation Herbert Quandt.

September 17, 2020

The recording is accessible at:
https://www.atlanticcouncil.org/blogs/geotech-cues/event-recap-western-society-ii

As part of this event, panelists discussed how AI is rapidly becoming the next playing field for great-power competition between the United States and China. Worried about losing out, countries and state conglomerates around the world have begun pursuing

[264] GeoTech Center, "Event recap | Western society at the crossroads, part II: Smart partnerships in a changing world," Atlantic Council, September 16, 2020, accessed March 26, 2021, https://www.atlanticcouncil.org/blogs/geotech-cues/event-recap-western-society-ii/.

their own policy regimes and strive for digital sovereignty, but many express a hesitancy to pick sides.

Over the course of the past year, experts from the Atlantic Council's GeoTech Center organized meetings in Paris, Brussels, and Berlin; traveled to Beijing and Shanghai; and held virtual conferences with participants in India and Africa, while working to address two questions: What are the geopolitical implications of emerging technologies and how can countries build smart partnerships amid the widening gyre?

The event concluded that:

- Entrepreneurs are not focused on diplomatic relations between countries. Their priority is to make partnerships and profits for their company. Thus, nations could work with these companies in efforts to engage Asia in building partnerships involving data and AI.
- Nations can best encourage entrepreneurs to work together by accepting one another's cultural values and mindsets and by talking with each other, not about each other. By making an effort to be inclusive, nations and private enterprises are able to find common interests to keep technology business cooperative. Including Chinese leaders in this series of exchanges is an ideal next step to developing a positive business relationship.
- India, as a democracy and in close proximity to China, has attempted to play the role of broker between the United States and China. However, it has been difficult because of rising tensions and border clashes with China. India is now looking to play less of a role.
- Immigration is key when making sure that we do not widen the divide between nations. It is to the advantage of the United States to have international talent contributing in the country, so easing restrictions on immigration is beneficial. Additionally, encouraging US students to study in China helps build business relationships.

5. Transatlantic Cooperation in the Era of AI[265]

Panelists: Mircea Geoană, NATO deputy secretary general; Kim Jørgensen, head of Cabinet, Cabinet of Executive Vice-President Margrethe Vestager, European Commission; Eric Schmidt, chairman of the National Security Commission on Artificial Intelligence (NSCAI); and Robert O. Work, NSCAI vice chair.

[265] Atlantic Council, "Transatlantic cooperation in the era of AI," Atlantic Council, October 28, 2020, accessed March 26, 2021, https://www.atlanticcouncil.org/event/transatlantic-cooperation-in-the-era-of-ai/.

October 28, 2020

The recording is accessible at:
https://www.atlanticcouncil.org/event/transatlantic-cooperation-in-the-era-of-ai/

Panelists discussed the future of the transatlantic relationship with respect to cooperation on artificial intelligence (AI), how best to promote shared values in the field, and what modern technologies mean in the defense and security context for European and US stakeholders.

In its Third Quarter Recommendations to the US Congress, the National Security Commission on Artificial Intelligence (NSCAI) proposed a Strategic Dialogue for Emerging Technologies (SDET) between the United States and the European Union. It encourages US policy makers to develop concrete actions to expand collaborative efforts and align transatlantic partners. In its March 2021 final report, NSCAI will build on these proposals to identify specific dialogue areas, which may include joint research and development (R&D) efforts and the development of privacy-enhancing AI applications, data sharing to facilitate cross-border projects, alignment of regulatory frameworks, coordinated investments in emerging technologies, facilitation of talent exchanges, and countering disinformation as well as intellectual property theft.

The event concluded that:

- The transatlantic relationship has produced extraordinary economic growth, military and national security, and cultural enrichment which has benefited citizens on both sides of the Atlantic. However, parties on both sides need to build a new partnership around AI since it is the most powerful tool in generations and all fundamental future accomplishments around science and engineering will have AI as a common denominator.
- Fostering a transatlantic talent ecosystem around AI, nurturing digital skills, and building a significant pool of “innovation champions” is a key priority. In line with the conclusions of NATO’s December 2019 summit in London and the European Commission’s “White Paper on Artificial Intelligence” released in February 2020, the transatlantic partner nations should build a road map for emerging disruptive technologies, including AI and big data, first-class connectivity, quantum computing, biotechnology, human enhancement, new materials, and space. In constructing this road map for emerging disruptive technologies, the partner nations should
    - Maintain a balance between traditional ways of deterrence and defense, while making a rapid and systematic transition to a new era of emerging technologies.

- Develop a balance between private and public initiatives and promote the transfer of best practices between government, private sector, and academia in order to accelerate innovation and discovery.
- Pursue all these initiatives by finding the common goals and interests across the North Atlantic community. At the same time, build respect for the existing differences of approach between a more regulatory environment in Europe and, in the United States, an ecosystem that gives preference to self-regulatory forces and that has a greater focus on defense-related issues.

6. Tech-Enabled Dis- and Misinformation, Social Platforms, and Geopolitics[266]

Panelists: Pablo Breuer, nonresident fellow with the Atlantic Council's GeoTech Center and CISO of Helm Services; Rose Jackson, director of the Policy Initiative at the Atlantic Council's Digital Forensic Research Lab; and Sara-Jayne Terp, nonresident senior fellow with the Atlantic Council's GeoTech Center.

February 3, 2021

The recording is accessible at:
https://www.atlanticcouncil.org/blogs/geotech-cues/event-recap-tech-enabled-dis-and-misinformation/

As part of this event, the Atlantic Council's GeoTech Center and Digital Forensics Research Lab examined the influence of new technologies on dis- and misinformation via social media platforms, while discussing the various challenges caused by the era of the "free Internet" and social media's ability to provide a mass audience with unchecked, unregulated content.

Increased Internet access worldwide and the caveats on its expansion have helped propagate dis- and misinformation. In parallel, the lack of regulation of online communities and content creation has created massive echo chambers, shifting the way society operates. Due to this conflictive context, the public and federal lawmakers have put under scrutiny the role of free Internet and the growth of targeted advertisements in the social media business model. In particular, they are now questioning this model's financial incentives and its role in the expanding reach and harm caused by misinformation.

[266] Sana Moazzam, "Event recap | Tech-enabled dis- and misinformation, social platforms, and geopolitics," Atlantic Council, February 3, 2021, accessed March 26, 2021, https://www.atlanticcouncil.org/blogs/geotech-cues/event-recap-tech-enabled-dis-and-misinformation/.

Finally, panelists discussed the future of privacy and its newfound placement as a luxury product, where companies like Apple and ProtonMail have begun selling privacy and security as a feature to set themselves apart in an era of mass data collection.

The event concluded that:

- Social media users must be informed about how much of their data is actually collected and what it is used for.
- In Western nations, social media is treated much like the news media and should consequently be held to the same regulations that journalistic outlets are held to in order to ensure truthful information.
- In the relationships between privacy, democracy, and disinformation, increased security could drastically reduce content targeting, while there must be constructive efforts to combat disinformation by educating users, taking down botnets, and emphasizing transparency. In addition, acknowledging the presence of information deserts and working to eliminate them could prevent disinformation from filling the gap. Sophisticated techniques, such as utilizing advertisements in disinformation spaces to provide a diversified range of views, could also prove effective in altering radicalized echo chambers.
- There is a need to reestablish a US Information Agency through public-private partnership and create more applicable constraints and regulations. With technology rapidly improving and accelerating, achieving digital literacy is imperative for society. This would help the government get ahead of growing challenges and tackle its reputation for creating laws and regulating only after an incident has occurred.
- More broadly, although counter misinformation efforts are going in the right direction, they must, however, improve faster and continue to provide effective outcomes.

Appendix F. Additional Readings

Marshall McLuhan, Quentin Fiore, and Shepard Fairey (Illustrator), *The Medium is the Massage* (United Kingdom: Penguin Books, 1967).

Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge University Press, 2015).

Yuval Noah Harari, *21 Lessons for the 21st Century* (United States: Spiegel & Grau; United Kingdom: Jonathan Cape, 2018).

Jared Diamond, *Guns, Germs and Steel: The Fate of Human Societies* (W. W. Norton & Company, 1997).

Annie Jacobsen, *The Pentagon's Brain: An Uncensored History of DARPA, America's Top-Secret Military Research Agency* (Little, Brown and Company, 2015).

Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (Doubleday, 1989).

Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order* (Houghton Mifflin Harcourt, 2018).

Mariana Mazzucato, *The Entrepreneurial State: Debunking Public vs. Private Sector Myths* (Anthem Press, 2013).

Richard A. Muller, *Physics for Future Presidents: The Science Behind the Headlines* (W. W. Norton & Company, 2008).

Acronyms

AI	artificial intelligence
APL	Approved Product List
AS	autonomous system
BGP	Border Gateway Protocol
CAIAC	Collective and Augmented Intelligence Against COVID-19
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CDC	Centers for Disease Control and Prevention
CDM	Continuous Diagnostics and Mitigation
CET	critical and emerging technologies
CEPI	Coalition for Epidemic Preparedness Innovations
CFIUS	Committee on Foreign Investment in the United States
CFO	chief financial officer
CHIPS Act	Creating Helpful Incentives to Produce Semiconductors for America Act
CIA	Central Intelligence Agency
CIO	chief information officer
CISA	Cybersecurity and Infrastructure Security Agency
CMMC	Cybersecurity Maturity Model Certification
COPUOS	United Nations Committee on the Peaceful Uses of Outer Space
CRISPR	Clustered Regularly Interspaced Short Palindromic Repeats
CUI	controlled unclassified information
DARPA	Defense Advanced Research Projects Agency
DCT	digital contact tracing

DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoC	Department of Commerce
DoD	Department of Defense
DoDIN	Department of Defense Information Network
EIOS	Epidemic Intelligence from Open Sources
EO	executive order
EU	European Union
FASC	Federal Acquisition Security Council
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDA	Food and Drug Administration
FedRAMP	Federal Risk and Authorization Management Program
FEMA	Federal Emergency Management Agency
FIMS	federated identity management system
FIPS	Federal Information Processing Standards
FIRRMA	Foreign Investment Risk Review Modernization Act of 2018
FISMA	*Federal Information Security Modernization Act of 2014*
GAO	Government Accountability Office
GDP	gross domestic product
GDPR	General Data Protection Regulation
GIS	geographic information system
GPAI	Global Partnership on Artificial Intelligence
GSA	General Services Administration
HHS	Department of Health and Human Services

HIC	high-income countries
HIPAA	Health Insurance Portability and Accountability Act
ICT	*information and communications technology*
IEC	International Electrotechnical commission
IHR	International Health Regulations
IP	Internet Protocol
IR	international relations
ISACs	Information Sharing and Analysis Centers
ISAO	Information Sharing and Analysis Organizations
ISO	International Organization for Standardization
IT	information technology
LEO	low Earth orbit
LMIC	low- and middle-income countries
LTS	long term sustainability
mRNA	messenger RNA
NAND	(NOT-AND) is a logic gate
NASA	National Aeronautics and Space Administration
NCATS	National Cybersecurity Assessment and Technical Services
NCEFOA	National Center for Epidemic Forecasting and Outbreak Analytics
NDAA	National Defense Authorization Act
NDN	named data network, or named data networking
NEON	National Ecological Observatory Network
NGA	National Geospatial-Intelligence Agency
NGO	nongovernmental organization
NICE	National Initiative for Cybersecurity Education

NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSCAI	National Security Commission on Artificial Intelligence
NSF	National Science Foundation
NSTC	National Science and Technology Council
NTIA	National Telecommunications and Information Administration
OMB	Office of Management and Budget
OST	Outer Space Treaty
OSTP	Office of Science and Technology Policy
OT	operational technology
PPD	Presidential Policy Directive
PPE	personal protective equipment
PPP	public-private partnership
PREDICT	a project of USAID’s Emerging Pandemic Threats program
QC	quantum cryptography
QEDC	Quantum Economic Development Consortium
QIS	quantum information science
QKD	quantum key distribution
R&D	research and development
S&T	science and technology
SAGE	Strategic Advisory Group of Experts on Immunization
SAML	Security Assertion Markup Language
SBoM	Software Bill of Materials
SCRM	supply chain risk management

SDG	Sustainable Development Goal
STEM	science, technology, engineering, and mathematics
TCBMs	transparency and confidence-building measures
TS/SCI	Top Secret/Sensitive Compartmented Information
UHC	Universal Health Coverage
UK	United Kingdom
UN	United Nations
UNOOSA	United Nations Office for Outer Space Affairs
USAID	United States Agency for International Development
USDA	United States Department of Agriculture
USG	United States government
USMCA	the United States-Mexico-Canada Free Trade Agreement
VEP	Vulnerabilities Equities Process
WHO	World Health Organization

Biographies of the GeoTech Commission Co-Chairs and Commissioners

Co-chairs

John Goodman, Chief Executive Officer, Accenture Federal Services

John Goodman is the Chief Executive of Accenture Federal Services (AFS), which serves clients across all sectors of the US federal government - defense, intelligence, public safety, health, and civilian. Since joining Accenture in 1998, he has held a variety of leadership roles - including managing director of Accenture's Defense & Intelligence portfolio, head of Management Consulting for the global Public Service Operating Group, and most recently Chief Operating Officer of AFS. John began his career at Accenture as a Member of the Communications & High Technology practice.

Prior to joining Accenture, John served for five years in the federal government as Deputy Under Secretary of Defense (Industrial Affairs & Installations), Deputy Assistant Secretary of Defense (Industrial Affairs), and a member of the staff of the National Economic Council, the White House office responsible for coordination of economic policy. He previously served on the Harvard Business School faculty.

John is co-chair of the Atlantic Council's GeoTech Commission and member of the boards of both the Atlantic Council and the Northern Virginia Technology Council, as well as a member of the Council on Foreign Relations. He is a member, and the immediate past chair, of the Executive Committee of the Professional Services Council, a former member of the Executive Committee of AFCEA, and the former chairman of the Defense Business Board. John was named Executive of the Year by the Greater Washington Government Contractors in 2018; a Wash100 inductee in 2018, 2019, 2020 and 2021; and a Fed100 Award winner in 2015. He has been awarded the Office of the Secretary of Defense Medal for Exceptional Public Service, the Department of Defense Medal for Distinguished Public Service, and the Department of Defense Medal for Outstanding Public Service.

John received his Bachelor of Arts, summa cum laude, from Middlebury College and his Master of Arts and Ph.D. from Harvard University.

Teresa Carlson, President and Chief Growth Officer, Splunk

As President and Chief Growth Officer at Splunk, Teresa Carlson leads our efforts to align and drive our ongoing business transformations across Splunk's go-to-market segments. Most recently, Carlson served as Vice President, Worldwide Public Sector and Industries, for Amazon Web Services (AWS). After she founded AWS's Worldwide Public Sector in 2010, Carlson's role eventually expanded to include financial services, energy services, telecommunications, and aerospace and services industry business units.

Carlson has also been a strong advocate for empowering women in the technology field. That passion led to the creation of "We Power Tech," AWS's diversity and inclusion initiative, which aims to ensure underrepresented groups – including women – are reflected throughout all AWS outreach efforts. Carlson dedicates time to philanthropic and leadership roles in support of the global community. Prior to joining AWS in 2010, Carlson led sales, marketing and business development organizations at Microsoft, Keyfile/Lexign and NovaCare. Carlson holds a B.A. and M.S. from Western Kentucky University.

Honorary Co-Chairs

Mark R. Warner, U.S. Senator from Virginia

Senator Warner was elected to the U.S. Senate in November 2008 and reelected to a third term in November 2020. He serves on the Senate Finance, Banking, Budget, and Rules Committees as well as the Select Committee on Intelligence, where he is the Chairman. During his time in the Senate, Senator Warner has established himself as a bipartisan leader who has worked with Republicans and Democrats alike to cut red tape, increase government performance and accountability, and promote private sector innovation and job creation. Senator Warner has been recognized as a national leader in fighting for our military men and women and veterans, and in working to find bipartisan, balanced solutions to address our country's debt and deficit.

From 2002 to 2006, he served as Governor of Virginia. When he left office in 2006, Virginia was ranked as the best state for business, the best managed state, and the best state in which to receive a public education.

The first in his family to graduate from college, Mark Warner spent 20 years as a successful technology and business leader in Virginia before entering public office. An early investor in the cellular telephone business, he co-founded the company that became Nextel and invested in hundreds of start-up technology companies that created tens of thousands of jobs.

Senator Warner and his wife Lisa Collis live in Alexandria, Virginia. They have three daughters.

Rob Portman, U.S. Senator for Ohio

Rob Portman is a United States Senator from the state of Ohio, a position he has held since he was first elected in 2010. Portman previously served as a U.S. Representative, the 14th United States Trade Representative, and the 35th Director of the Office of Management and Budget (OMB). In 1993, Portman won a special election to represent Ohio's 2nd congressional district in the U.S. House of Representatives and served six terms before President George W. Bush appointed him as U.S. Trade Representative in May 2005. Portman currently serves as the Ranking Member on the Senate Homeland Security and Governmental Affairs Committee, as well as on the Senate Finance and Foreign Relations Committees. He was born and raised in Cincinnati, where he still lives today with his wife Jane. Together they have three children: Jed, Will, and Sally.

Suzan DelBene, U.S. Congresswoman Representing Washington's 1st District

Congresswoman Suzan DelBene represents Washington's 1st Congressional District, which spans from northeast King County to the Canadian border and includes parts of King, Snohomish, Skagit, and Whatcom counties. First sworn into the House of Representatives in November 2012, Suzan brings a unique voice to the nation's capital with more than two decades of experience as a successful technology entrepreneur and business leader. Suzan takes on a wide range of challenges both in Congress and in the 1st District and is a leader on issues of technology, health care, trade, taxes, environmental conservation, and agriculture.

Suzan currently serves as the Vice Chair on the House Ways and Means Committee, which is at the forefront of debate on a fairer tax code, health care reform, trade deals, and lasting retirement security. She serves on the Select Revenue Measures and Trade Subcommittees. Suzan also serves as Chair of the forward-thinking New Democrat Coalition, which is one of the largest ideological coalitions in the House, and is co-chair of the Women's High Tech Caucus, Internet of Things Caucus, and Dairy Caucus. She is also a member of the Pro-Choice Caucus.

Over more than two decades as an executive and entrepreneur, she helped to start drugstore.com as Vice President of Marketing and Store Development, and served as CEO and President of Nimble Technology, a business software company based on technology developed at the University of Washington. Suzan also spent 12 years at Microsoft, most recently as corporate vice president of the company's mobile communications business.

Before being elected to Congress, Suzan served as Director of the Washington State Department of Revenue. During her tenure, she proposed reforms to cut red tape for small businesses. She also enacted an innovative tax amnesty program that generated $345 million to help close the state's budget gap while easing the burden on small businesses.

Suzan and her husband, Kurt DelBene, have two children, Becca and Zach, and a dog named Reily.

Michael T. McCaul, U.S. Congressman Representing Texas' 10th District

Congressman Michael T. McCaul is currently serving his ninth term representing Texas' 10th District in the United States Congress. The 10th Congressional District of Texas stretches from the city of Austin to the Houston suburbs and includes Austin, Bastrop, Colorado, Fayette, Harris, Lee, Travis, Washington and Waller Counties.

At the start of the 116th Congress, Congressman McCaul became the Republican Leader of the *Foreign Affairs* Committee. This committee considers legislation that impacts the diplomatic community, which includes the Department of State, the Agency for International Development (USAID), the Peace Corps, the United Nations, and the enforcement of the Arms Export Control Act. In his capacity as the committee's Republican Leader, McCaul is committed to ensuring we promote America's leadership on the global stage. In his view, it is essential the United States bolsters international engagement with our allies, counters the aggressive policies of our adversaries, and advances the common interests of nations in defense of stability and democracy around the globe. He will continue to use his national security expertise to work to counter threats facing the United States, especially the increasing threat we face from nation state actors such as China, Iran, Russia, North Korea, among others.

Prior to Congress, Michael McCaul served as Chief of Counter Terrorism and National Security in the U.S. Attorney's office, Western District of Texas, and led the Joint Terrorism Task Force charged with detecting, deterring, and preventing terrorist activity. McCaul also served as Texas Deputy Attorney General under current U.S. Senator John Cornyn, and served as a federal prosecutor in the Department of Justice's Public Integrity Section in Washington, DC.

A fourth generation Texan, Congressman McCaul earned a B.A. in Business and History from Trinity University and holds a J.D. from St. Mary's University School of Law. In 2009 Congressman McCaul was honored with St. Mary's Distinguished Graduate award. He is also a graduate of the Senior Executive Fellows Program of the School of Government, Harvard University. Congressman McCaul is married to his wife, Linda. They are proud parents of five children: Caroline, Jewell, and the triplets Lauren, Michael, and Avery.

Commissioners

Max R. Peterson II, Vice President, Worldwide Public Sector, Amazon Web Services

Max Peterson is Vice President for Amazon Web Services' (AWS) Worldwide Public Sector. In this role, Max supports public sector organizations as they leverage the unique advantages of commercial cloud to drive innovation among government, educational institutions, health care institutions, and nonprofits around the world.

A public sector industry veteran with thirty years of experience, he has an extensive background in developing relationships with public sector customers. He has previously worked with Dell Inc. as Vice President and General Manager for Dell Federal Civilian and Intelligence Agencies, as well as CDWG and Commerce One.

Max earned both a Bachelor's Degree in Finance and Master's of Business Administration in Management Information Systems from the University of Maryland.

Paul Daugherty, Accenture Chief Executive – Technology and Chief Technology Officer

Paul Daugherty is Accenture's Group Chief Executive – Technology & Chief Technology Officer. He leads all aspects of Accenture's technology business. Paul is also responsible for Accenture's technology strategy, driving innovation through R&D in Accenture Labs and leveraging emerging technologies to bring the newest innovations to clients globally. He recently launched Accenture's Cloud First initiative to further scale the company's market-leading cloud business and is responsible for incubating new businesses such as blockchain, extended reality and quantum computing. He founded and oversees Accenture Ventures, which is focused on strategic equity investments and open innovation to accelerate growth. Paul is responsible for managing Accenture's alliances, partnerships and senior-level relationships with leading and emerging technology companies, and he leads Accenture's Global CIO Council and annual CIO and Innovation Forum. He is a member of Accenture's Global Management Committee.

Maurice Sonnenberg, Guggenheim Securities

Maurice Sonnenberg has served as an outside advisor to five Presidential Administrations in the areas of international trade, finance, international relations, intelligence, and foreign election monitoring. In 1994 and 1995, he served as a member of the US Commission on Protecting and Reducing Government Secrecy, and from 1996 as the Senior Advisor to the US Commission on the Roles and Capabilities of the US Intelligence Community. He was a member of the President's Foreign Intelligence Advisory Board under President Bill Clinton for 8 years. In 2002, he was a member of the Task

Force of Terrorist Financing for the Council on Foreign Relations. From 2007-2010, he served on the Department of Homeland Security Advisory Council and the Panel Advisory Board for the Secretary of the Navy from 2008-2015. In 2012-14, he served as co-Chairman of the National Commission for the Review of the Research and Development Programs for the Intelligence Community. He has also served as an Official US Observer at elections in Latin America. This includes multiple elections in El Salvador, Guatemala, Nicaragua and Mexico. Sonnenberg has worked at the investment banking firms Donaldson Lufkin and Jenrette, Bear Stearns, and J.P. Morgan, and at the law firms Hunton & Williams, Manatt, Phelps & Phillips. Currently, he is with Guggenheim Securities as Senior International Advisor. He is also a Senior Advisor to the Advanced Metallurgical Group, N.V.

Michael Chertoff, Former U.S. Secretary of Homeland Security

Michael Chertoff is the Executive Chairman and Co-Founder of The Chertoff Group. From 2005 to 2009, he served as Secretary of the U.S. Department of Homeland Security. Earlier in his career, Mr. Chertoff served as a federal judge on the U.S. Court of Appeals for the Third Circuit and head of the U.S. Department of Justice's Criminal Division. He is the Chairman of the Board of Directors of BAE Systems, Inc., the U.S.-based subsidiary of BAE Systems plc. In 2018, he was named the chairman of the Board of Trustees for Freedom House. He currently serves on the board of directors of Noblis and Edgewood Networks. In the last five years, Mr. Chertoff co-chaired the Global Commission in Stability of Cyberspace and also co-chairs the Transatlantic Commission on Election Integrity. Chertoff is magna cum laude graduate of Harvard College and Harvard Law School.

Michael J. Rogers, Former Chairman of the U.S. House Permanent Select Committee on Intelligence

Mike Rogers is a former member of Congress, where he represented Michigan's Eighth Congressional District for seven terms. While in the U.S. House of Representatives, he chaired the powerful House Permanent Select Committee on Intelligence (HPSCI), authorizing and overseeing a budget of $70 billion that funded the nation's seventeen intelligence agencies. Mr. Rogers built a legacy as a bipartisan leader on cybersecurity, counterterrorism, intelligence, and national security policy. Mr. Rogers worked with two presidents, congressional leadership, and countless foreign leaders, diplomats, and intelligence professionals. Before joining Congress, he served as an officer in the US Army and as a Special Agent with the FBI. He is currently investing in and helping build companies that are developing solutions for healthcare, energy efficiency, and communications challenges. He also serves as a regular national security commentator on CNN and hosted the channel's documentary-style original series *Declassified*.

Mr. Rogers is a regular public speaker on global affairs, cybersecurity, and leadership. He is married to Kristi Rogers and has two children.

Pascal Marmier, Head, Economy of Trust Foundation, SICPA

Pascal Marmier is head of SICPA's Economy of Trust Foundation. Most recently, Marmier held several positions in the United States within Swiss Re, a global reinsurer, focusing on digital strategy and innovation management. Previously, he spent twenty years as a Swiss diplomat as one of the early leaders of the Swissnex network, a private–public partnership dedicated to facilitating collaboration with Swiss universities, startups, and corporations in all fields related to science, technology, and innovation. After spending a decade establishing key partnerships and activities in Boston, Marmier moved to China to establish the Swissnex platform in the region. He holds law degrees from the University of Lausanne and Boston University, as well as an MBA from the MIT Sloan School of Management.

Ramayya Krishnan, PhD, Director, Block Center for Technology and Society, Carnegie Mellon University

Ramayya Krishnan is the W. W. Cooper and Ruth F. Cooper Professor of Management Science and Information Systems at Carnegie Mellon University. He is Dean of the H. John Heinz III College of Information Systems and Public Policy and directs the Block Center for Technology and Society at the university. His scholarly contributions have focused on mathematical modeling of organizational decision making, the design of data driven decision support systems and statistical models of consumer behavior in digital environments. He advises governments, businesses and development banks on digital transformation technology and its consequences.

Dr. Shirley Ann Jackson, President, Rensselaer Polytechnic Institute

The Honorable Shirley Ann Jackson, Ph.D., has served as the 18th president of Rensselaer Polytechnic Institute since 1999. A theoretical physicist described by Time Magazine as "perhaps the ultimate role model for women in science," Dr. Jackson has held senior leadership positions in academia, government, industry, and research. She is the recipient of many national and international awards, including the National Medal of Science, the United States' highest honor for achievement in science and engineering. Dr. Jackson served as Co-Chair of the United States President's Intelligence Advisory Board from 2014 to 2017 and as a member of the President's Council of Advisors on Science and Technology from 2009 to 2014. Before taking the helm at Rensselaer, she was Chairman of the U.S. Nuclear Regulatory Commission from 1995 to 1999. She serves on the boards of major corporations that include FedEx and PSEG, where she is Lead Director.

Dr. Jackson holds an S.B. in Physics, and a Ph.D. in Theoretical Elementary Particle Physics, both from MIT.

Susan M. Gordon, Former Principal Deputy Director of National Intelligence

The Honorable Susan (Sue) M. Gordon served as Principal Deputy Director of National Intelligence from August 2017 until August 2019. In her more than three decades of experience in the IC, Ms. Gordon served in a variety of leadership roles spanning numerous intelligence organizations and disciplines, including serving as the Deputy Director of the National Geospatial-Intelligence Agency (NGA) from 2015 to 2017. In this role, she drove NGA's transformation to meet the challenges of a 21st century intelligence agency. Since leaving government service, Ms. Gordon serves on a variety of public and private boards, is a fellow at Duke and Harvard Universities, and consults with a variety of companies on technology—including cyber and space—strategy, and leadership, focusing on shared responsibility for national and global security.

Vint Cerf

Vinton G. Cerf is vice president and Chief Internet Evangelist for Google. Cerf is the codesigner of the TCP/IP protocols and the architecture of the Internet. He has served in executive positions at the Internet Corporation for Assigned Names and Numbers, the Internet Society, MCI, the Corporation for National Research Initiatives, and the Defense Advanced Research Projects Agency. A former Stanford Professor and member of the National Science Board, he is also the past president of the Association for Computing Machinery and serves in advisory capacities at the National Institute of Standards and Technology, the Department of Energy, and the National Aeronautics and Space Administration. Cerf is a recipient of numerous awards for his work, including the US Presidential Medal of Freedom, US National Medal of Technology, the Queen Elizabeth Prize for Engineering, the Prince of Asturias Award, the Tunisian National Medal of Science, the Japan Prize, the Charles Stark Draper Prize, the ACM Turing Award, the Legion d'Honneur, the Franklin Medal, Foreign Member of the British Royal Society and Swedish Academy of Engineering, and twenty-nine honorary degrees. He is a member of the Worshipful Company of Information Technologists and the Worshipful Company of Stationers.

Zia Khan, PhD, Vice President for Innovation, The Rockefeller Foundation

As Senior Vice President for Innovation, Zia Khan oversees the Rockefeller Foundation's approach to developing solutions that can have a transformative impact on people's lives through the use of convenings, data and technology, and strategic partnerships. He writes and speaks frequently on leadership, strategy, and innovation. Khan has served on the World Economic Forum Advisory Council for Social Innovation and the

US National Advisory Board for Impact Investing. He leads a range of the Rockefeller Foundation's work in applying data science for social impact and ensuring artificial intelligence contributes to an inclusive and equitable future.

Prior to joining the Rockefeller Foundation, Khan was a management consultant advising leaders in technology, mobility, and private equity sectors. He worked with Jon Katzenbach on research related to leadership, strategy, and organizational performance, leading to their book, *Leading Outside the Lines*.

Zia holds a BS from Cornell University and MS and PhD from Stanford University.

Anthony Scriffignano, PhD, Senior Vice President, Chief Data Scientist at Dun & Bradstreet Corporation

Anthony Scriffignano, PhD is Senior Vice President, Chief Data Scientist at Dun & Bradstreet Corporation. He is an internationally recognized data scientist with experience spanning over forty years in multiple industries and enterprise domains. Scriffignano has extensive background in advanced anomaly detection, computational linguistics and advanced inferential algorithms, leveraging that background as primary inventor on multiple patents worldwide. Scriffignano was recognized as the U.S. Chief Data Officer of the Year 2018 by the CDO Club, the world's largest community of C-suite digital and data leaders. He is also a member of the OECD Network of Experts on AI working group on implementing Trustworthy AI, focused on benefiting people and the planet. He has briefed the US National Security Telecommunications Advisory Committee and contributed to three separate reports to the president, on Big Data Analytics, Emerging Technologies Strategic Vision, and Internet and Communications Resilience. Additionally, Scriffignano provided expert advice on private sector data officers to a group of state Chief Data Officers and the White House Office of Science and Technology Policy. Scriffignano serves on various advisory committees in government, private sector, and academia. Most recently, he has been called upon to provide insight on data science implications in the context of a highly disrupted datasphere and the implications of the global pandemic. He is considered an expert on emerging trends in advanced analytics, the "Big Data" explosion, artificial intelligence, multilingual challenges in business identity and malfeasance in commercial and public-sector contexts.

Frances F. Townsend, Executive Vice President, Activision Blizzard

Frances Fragos Townsend is the Executive Vice President of Corporate Affairs, Chief Compliance Officer and Corporate Secretary at Activision Blizzard. Prior to that, she was Vice Chairman, General Counsel and Chief Administration Officer at MacAndrews & Forbes, Inc. In her 10 years there, she focused internally on financial, legal and personnel issues, as well as international, compliance and business development across

MacAndrews' portfolio companies. Prior to that, she was a corporate partner with the law firm of Baker Botts, LLP. From 2004 to 2008, Ms. Townsend served as Assistant to President George W. Bush for Homeland Security and Counterterrorism and chaired the Homeland Security Council. She also served as Deputy National Security Advisor for Combatting Terrorism from 2003 to 2004. Ms. Townsend spent 13 years at the US Department of Justice under the administrations of President George H. W. Bush, President Bill Clinton and President George W. Bush. She has received numerous awards for her public service accomplishments. Ms. Townsend is a Director on the Board of two public companies: Chubb and Freeport McMoRan. She previously served on the Boards at Scientific Games, SciPlay, SIGA and Western Union. She is an on-air senior national security analyst for CBS News. Ms. Townsend previously served on the Director of National Intelligence's Senior Advisory Group, the Central Intelligence Agency's (CIA) External Advisory Board and the US President's Intelligence Advisory Board. Ms. Townsend is a trustee on the Board of the New York City Police Foundation, the Intrepid Sea, Air & Space Museum, the McCain Institute, the Center for Strategic and International Studies (CSIS) and the Atlantic Council. She also serves on the Board at the Council on Foreign Relations, on the Executive Committee of the Trilateral Commission and the Board of the International Republican Institute. She is a member of the Aspen Strategy Group.

Admiral James Stavridis, USN, Ret.

Admiral James Stavridis is an Operating Executive of The Carlyle Group and Chair of the Board of Counselors of McLarty Global Associates, following five years as the 12th Dean of The Fletcher School of Law and Diplomacy at Tufts University. He also serves as the Chairman of the Board of the Rockefeller Foundation. A retired four-star officer in the U.S. Navy, he led the North Atlantic Treaty Organization (NATO) Alliance in global operations from 2009 to 2013 as Supreme Allied Commander with responsibility for Afghanistan, Libya, the Balkans, Syria, counter piracy and cyber security. He also served as Commander of U.S. Southern Command, with responsibility for all military operations in Latin America from 2006 to 2009. He earned more than 50 medals, including 28 from foreign nations in his 37-year military career. Admiral Stavridis earned a PhD in international relations and has published 10 books and hundreds of articles in leading journals around the world, including the recent novel "2034: A Novel of the Next World War," which was a *New York Times* bestseller. His 2012 TED Talk on global security has close to one million views. Admiral Stavridis is a monthly columnist for TIME Magazine and Chief International Security Analyst for NBC News.

Biographies of Supporting Atlantic Council Staff

Dr. David A. Bray, Director, GeoTech Center, Atlantic Council

Dr. David A. Bray has served in a variety of leadership roles in turbulent environments, including bioterrorism preparedness and response from 2000 to 2005, time on the ground in Afghanistan in 2009, serving as a non-partisan Senior National Intelligence Service Executive directing a bipartisan National Commission for the Review of the Research and Development Programs of the US Intelligence Community, and providing leadership as a non-partisan federal agency Senior Executive where he led a team that received the global CIO 100 Award twice in 2015 and 2017. He is an Eisenhower Fellow, Marshall Memorial Fellow, and Senior Fellow with the Institute for Human & Machine Cognition. *Business Insider* named him one of the top "24 Americans Who Are Changing the World" and the World Economic Forum named him a Young Global Leader. Over his career, he has advised six different start-ups, led an interagency team spanning sixteen different agencies that received the National Intelligence Meritorious Unit Citation, and received the Joint Civilian Service Commendation Award, the National Intelligence Exceptional Achievement Medal, Arthur S. Flemming Award, as well as the Roger W. Jones Award for Executive Leadership. He is the author of more than forty academic publications, was invited to give the AI World Society Distinguished Lecture to the United Nations in 2019, and was named by HMG Strategy as one of the Global "Executives Who Matter" in 2020.

Dr. Peter Brooks, Consultant, GeoTech Center, Atlantic Council

Peter Brooks is a senior researcher and national security analyst at the Institute for Defense Analyses, a federally funded research and development center. For more than three decades, he has contributed to the understanding of critical national security issues for a wide range of government agencies. His broad expertise includes intelligence analysis, advanced technologies and applications, and joint force analyses, experimentation, strategy, and cost assessments.

Stephanie Wander, Deputy Director, GeoTech Center, Atlantic Council

Stephanie Wander is a technology and innovation strategist with a successful track record of launching large-scale projects to solve global grand challenges. Ms. Wander's approaches integrate innovation best practices and mindsets, including design thinking, behavior change strategies, foresight techniques, and expert and public crowdsourcing.

Previously, Ms. Wander was a lecturer at the University of Southern California Suzanne Dworak-Peck School of Social Work where she taught graduate social work professionals in design, innovation, and disruptive technology.

Rose Butchart, Senior Adviser, National Security Initiatives, GeoTech Center, Atlantic Council

Rose Butchart is the senior adviser for National Security Initiatives at the Atlantic Council's GeoTech Center.

As a program manager for the Department of Defense's National Security Innovation Network, she managed, designed, and scaled a variety of programs, including a technology, transfer, and transition (T3) program designed to bring breakthrough Department of Defense lab technology to market— and to the warfighter. She also managed a workshop series to tackle some of the military's intractable problems and a fellowship which placed active duty military and Department of Defense civilians at technology start-ups.

Claudia Vaughn Zittle, Program Assistant, Atlantic Council GeoTech Center

Claudia Vaughn Zittle was a program assistant with the Atlantic Council's GeoTech Center. In this role, she managed a wide range of projects at the intersection of emerging technologies and dynamic geopolitical landscapes. She also conducted research and provided written analysis for publication on Atlantic Council platforms.

Originally from the Washington, DC, area, she received her BA in International Relations from Cornell College. She is continuing her education at American University's School of International Service, where she studies International Relations with a concentration in US Foreign Policy and National Security.

Claire Branley, Program Assistant, Atlantic Council GeoTech Center

Claire Branley joined the Atlantic Council's Geotech Center after graduating from the University of Washington with a BS in Public Health and Global Health. She was a research assistant in the Moussavi-Harami Lab, uncovering gene therapies for inherited heart disease. She is deeply passionate about the prevention of disease and has assisted several maternal and child health research projects and volunteered in farm-to-food pantry initiatives to decrease food insecurity in the Seattle area. Her interests include chronic disease burden, global food security, and promoting interdisciplinary solutions.

Biographies of the Key Contributors to the GeoTech Commission Report

Research and writing on misinformation

Dr. Pablo Breuer, Nonresident Senior Fellow, GeoTech Center, Atlantic Council

Dr. Pablo Breuer is an information/cyber warfare expert and a twenty-two-year veteran of the US Navy with tours including the National Security Agency, US Cyber Command, and United States Special Operations Command. He is a cofounder of the Cognitive Security Collaborative and coauthor of the Adversarial Misinformation and Influence Tactics and Techniques (AMITT) framework.

Dr. Robert Leonhard, National Security Analysis, Johns Hopkins University Applied Physics Laboratory

Robert Leonhard is on the principal professional staff as an analyst in the National Security Analysis Department of Johns Hopkins University's Applied Physics Laboratory (JHU/APL). His main areas of focus are irregular warfare, nuclear deterrence, and game design. Prior to joining JHU/APL, he earned a PhD in American History from West Virginia University, a Master of Military Arts and Sciences from the US Army, an MS in International Relations from Troy State University, and a BS in European History from Columbus University. He is a retired Army infantry officer and planner. He is the author of *The Art of Maneuver* (Presidio Press, 1991), *Fighting by Minutes: Time and the Art of War* (Praeger, 1994), *The Principles of War for the Information Age* (Presidio Press, 1998), *Little Green Men: a primer in Russian Unconventional Warfare, Ukraine 2013-2014* (JHUAPL, 2016), and *The Defense of Battle Position Duffer: Cyber-Enabled Maneuver in Multi-Domain Battle* (JHUAPL, 2016). He may be contacted at Robert.Leonhard@jhuapl.edu.

John Renda, Program Manager, Army Special Operations, Johns Hopkins University Applied Physics Laboratory

Col. John Renda, USA (Ret), is a program manager for Army Special Operations at the Johns Hopkins University's Applied Physics Laboratory. He graduated from Tulane University with a degree in Political Science and International Relations, and earned a MS in

National Security from the US Naval War College. He served as a career Psychological Operations officer in US Army Special Operations. His key assignments included 75th Ranger Regiment Information Operations Officer, 1st Psychological Operations Battalion Commander, United States Special Operations Command (USSOCOM) Director J39 National Capital Region, and National Security Council Staff, Director for Strategic Communication. He may be contacted at john.renda@jhuapl.edu.

Dr. Sara-Jayne Terp, Nonresident Senior Fellow, GeoTech Center, Atlantic Council

Sara-Jayne Terp builds frameworks to improve how autonomous systems, algorithms, and human communities work together. At Threet Consulting, she creates processes and technologies to support community-led disinformation defence. She is an Atlantic Council Senior Fellow, CogSecCollab lead, and chair at CAMLIS and Defcon AI Village. Her background includes intelligence systems, crowdsourced data gathering, autonomous systems (e.g., human-machine teaming), data strategy, data ethics, policy, nation state development, and crisis response.

Appendix B

Stewart Scott, Assistant Director, GeoTech Center, Atlantic Council

Stewart Scott is an assistant director with the Atlantic Council's GeoTech Center, where he conducts research and provides written analysis for publication on Atlantic Council platforms and works on joint projects with other centers in the Atlantic Council. He earned his AB, along with a minor in Computer Science, at the School of Public and International Affairs at Princeton University.

We would also like to thank the following members of the Atlantic Council's Cyber Statecraft Initiative for their contributions to Appendix B: **Trey Herr, Simon Handler, Madison Lockett, Will Loomis, Emma Schroeder,** and **Tianjiu Zuo**.

Appendix C and writings on global health

Dr. Divya Chander, Nonresident Senior Fellow, GeoTech Center, Atlantic Council

Divya Chander, MD, PhD is a physician-scientist, futurist, and entrepreneur (co-founder of 2 startups). She is a practicing anesthesiologist with specializations in neurosurgery, ENT, and critical care. As a data scientist with expertise in neural signal processing, she has developed algorithms to automate tracking of states of consciousness. Dr. Chander is also Chair of Neuroscience at Singularity University, a Silicon Valley think tank for data and technology acceleration, applications, and ethics. She serves as medical, science, and technology advisor to a number of companies in the medical, space life sciences, and neurotechnology spaces. Dr. Chander was named one of 2020's top digital health innovators by Intelligent Health AI. As Nonresident Senior Fellow at the Geotech Center, she collaborates to foster good data and technology policy choices for key stakeholders around the world in the area of data trusts, data security, public health, and pandemic resilience.

Appendix D

Inkoo Kang, Research Consultant, GeoTech Center, Atlantic Council

US Air Force 2nd Lt. Inkoo Kang is a research consultant for the Atlantic Council's GeoTech Center. At the Atlantic Council, he conducts research and provides written analyses on the increasingly important role of outer space for social, economic, and military operations. His main interest focuses on how emerging technologies are merging military, diplomatic, humanitarian, and economic challenges and how the military must learn to adapt to such threats.

Appendix E

Borja Prado, Research Assistant, GeoTech Center Atlantic Council

Borja Prado holds an MS in Foreign Service (MSFS) from Georgetown University, where he concentrated in Global Politics and Security, focusing on the impact of disruptive technologies on governments, businesses, and societies.

He aims to apply his research experience, language skills, and strong background in technology and global affairs to help governments, businesses, and societies succeed in this increasingly uncertain era.

Acknowledgements

We would like to thank the following members of the Commission Co-Chair teams for their assistance, expertise, and technical review of the report:

- **Stoney Burke**, Head of Federal Affairs and Public Policy, Amazon Web Services
- **Ira Entis**, Managing Director, Growth and Strategy Lead, Accenture Federal Services
- **Geoffrey Kahn**, Managing Director, Government Relations, Accenture
- **Pamela Merritt**, Managing Director, Federal Marketing and Communications, Accenture Federal Services
- **Davis Pace**, Professional Staff Member, House *Foreign Affairs* Committee
- **Sean Sweeney**, Manager, Government Relations, Accenture
- **Clayton Swope**, Senior Manager, National Security Public Policy, Amazon Web Services
- **Carolyn Vigil**, Senior Customer Engagement Manager, Amazon Web Services

We would like to acknowledge the following individuals for their review and commentary on relevant sections of the report: **Laura Bate, Natalie Barrett, Pablo Breuer, Mark Brunner, Mung Chiang, Kevin Clark, Donald Codling, Carol Dumaine, Ryan G. Faith, Melissa Flagg, James F. Geurts, Jasper Gilardi, Bob Gourley, Bob Greenberg, Simon Handler, Henry Hertzfeld, Robert Hoffman, Erich James Hösli, Diane M. Janosek, William Jeffrey, Charles Jennings, Declan Kirrane, John J. Klein, Sandra J. Laney, John Logsdon, Robert Lucas, Lauren Maffeo, Jerry Mechling, Ivan Medynskyi, Ben King, Ben Murphy and the team at Reaching the Future Faster LLC, James Olds, Nikhil Raghuveera, Matthew Rose, Benjamin Schatz, Emma Schroeder, Jeremy Spaulding, Keith Strier, Daniella Taveau, Trent Teyema, Bill Valdez,** and **Tiffany Vora**.

We also would like to express sincere appreciation to individuals both internal and external to the Atlantic Council for help in preparing this report for final publication. Their professional and dedicated efforts were essential to this work.

Lastly, we want to thank all the GeoTech Fellows and GeoTech Action Council members, each of whom embodies the spirit of the new Center as we look to the future ahead: **Be Bold. Be Brave. Be Benevolent.**

Commission on the Geopolitical Impacts of New Technologies and Data
Be Bold
Be Brave
Be Benevolent

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1030 15th Street, NW, 12th Floor,
Washington, DC 20005
(202) 778-4952
www.AtlanticCouncil.org

Two Examples of Positive Outcomes from AI Startups:

With Aidoc, a successful healthcare and AI company, have seen the success of solutions that sit atop hospital PACS and EHR systems, using FDA-cleared AI models to flag urgent findings such as stroke and pulmonary embolism. By proactively surfacing urgent cases and automating care coordination across the enterprise, these solutions help radiologists and care teams accelerate time-to-treatment, reduce diagnostic errors, and optimize clinical workflows. https://www.aidoc.com/

With Hippocratic AI, also a successful healthcare and AI company, have seen the success of non-diagnostic AI healthcare agents that engage patients via natural conversations (e.g., phone, chat) for low-risk care navigation, follow-ups, education, and administrative support. Our platform emphasizes patient safety, prevention, and empowerment as core design principles. https://www.hippocraticai.com/

These real-world applications demonstrate how AI can meaningfully transform care delivery.

I also would like to briefly acknowledge two individuals. One is Patricia Branch Coltrane, Virginia Science Teacher of the Year for her work at Warwick High School, a reflection of her tireless commitment to her students - who was my 9th grade AP biology teacher and without whom I wouldn't have had the opportunity to start working on computers, early AI prototypes, and the Internet back in 1993.

The second is Brian Finlay, President and Chief Executive Officer of the Stimson Center, a true champion of positive “change agents” who always has been willing to entertain creative ideas that get results for both policies and programs differently and better, given our changing world. He also steadfastly embodies non-partisanship when exploring the art of how to do things better locally and globally.

AI Services to Citizens in 2023 and Beyond

September 07, 2023

A group of NAPA Fellows associated with the Standing Panel on Technology Leadership recently released a call to action on responsibly using AI to benefit public service at all levels of government. We are grateful for the strong positive response to this call from numerous colleagues in governmental communities. We provide additional scoping observations below, and welcome continued and expanded dialogue on this critical issue.

Artificial Intelligence and Public Service: Key New Challenges

David Bray, PhD
Distinguished Fellow, Stimson Center as well as Business Executives for National Security

In May 2023, the Executive Office of the President announced actions to promote responsible AI innovation, having previously announced in October 2022 a "Blueprint for an AI Bill of Rights" to include safe and effective systems, protections against algorithmic discrimination, data privacy, notice and explanation, and alternative options to include opting-out of such systems. Such efforts raise interesting questions about (1) where can advances in AI improve delivery of Services to Citizens and (2) what changes in how public service organizes and operates are needed to make such improvements a reality?

I. Where can advances in AI improve delivery of Services to Citizens?

For FY2024 and FY2025, we can look to see signs of adoption of the following at the federal level of the U.S. government as well within state and local governments:

1. Increased use of AI-supported assistance for individuals seeking government information. For example, several cities already have “311” telephone lines and mobile apps to assist individuals with non-emergency city services as well as to provide information on programs, events, and activities in the city.
2. Increased use of AI-supported assistance for talent management and skills matching. AI will help community members find new jobs and tailor training to hone and improve their skills for upward mobility in their jobs.
3. Increased use of AI-supported review of public applications and filings. AI assistants will provide more tailored support to individuals, to better understand what they are applying for and pre-review a public application or filing prior to human approval.
4. Increased use of AI-supported legal, financial, and ethical reviews. An AI assistant will do the initial review, let an individual know if more information is required, and provide a preliminary result for final review by a human.
5. Increased use of AI-supported assistance for analyzing geospatial data. AI can assist in making sense of geospatial information— for example, data from drones for civilian purposes, private cube satellites, and sensors associated with the “internet of things” -- as well as identifying patterns of importance to improve the delivery of public services.

For the longer-term, beyond just two years, we can look to see improved Services to Citizens to include:

1. Use of AI-enabled delivery of materials and provision of transportation. This would allow public services to be paired with AI-enabled autonomous vehicles to include fire and emergency services.
2. Use of AI-enabled robots to offset repetitive and manually intensive work. This will include using AI for civil construction efforts, disaster response, healthcare, or other public functions.
3. Use of AI-enabled digital assistants to detect and help understand biases. AI will help hold up a

4. Use of AI-enabled "digital twins" of real-world dynamics. AI will allow public service organizations to build models of real-world dynamics—either of actual physical assets or social interactions. Such models will create highly accurate "digital twins" that would allow individuals in public service to experiment with certain scenarios in a digital environment.
5. Use of AI to match humans into different ad-hoc teams to fit a specific public service goal or problem set.

II. What changes in how public service organizes and operates are needed to make such improvements a reality?

Consistent with the goals of a "Blueprint for an AI Bill of Rights", public service needs to consider how to involve the public in a participatory process involving AI service deliver that does not become itself either an overly burdensome or politically fragmented process.

- Governments will need to implement something akin to "public review boards" that look at the diversity, consistency, and appropriateness of the data used.
- Public service will need to solve growing cybersecurity challenges, to include the growing challenges of disinformation and misinformation as these can erode the services of government agencies in ways akin to cyber-related disrupts too.
- AI cannot be treated as "bolt on" to existing efforts – true leadership is required to evaluate the why, what, and how associated with the mission sets of departments and how they interact with the public, with non-profits and businesses, and with other government partners.

In addition, public service will need to do extensive work on engagements with the public on how data is curated, used to train AI, and governed to ensure it is used responsibly, to include:

- Discussions of AI and Citizen Services cannot overlook the essentialness of data curation, training, and government associated with AI systems.
- Without diverse or consistent data, the AI trained by the data may make decisions that erode public trust.
- Without appropriate use of data, public trust may also erode. Such activities should involve outreach efforts by public service organizations, to increase both digital literacy and understanding of AI systems and what they can do.

III. How Can We Proceed in Advancing AI Services to Citizens in 2023 and Beyond?

Cumulatively, the points raised in the earlier two sections demonstrate that we cannot treat employment of AI Services to Citizens as "just" a technology issue – in fact improving AI and Citizen Service is best viewed as a collective set of process improvement, workforce transformation, and leadership decision-making challenges and opportunities to solve. Furthermore, we cannot sit on the sidelines as technology moves forward – we will have to "learn by doing". This includes specific Presidential-level AI projects ideally spanning multiple departments, with top leadership support, to ensure AI delivers Citizen Services more effectively than before.

To ensure public success, Presidential-level AI projects should include intentional work on whom to include in the governance and oversight of those AI and associated data systems as well as how to ensure the diversity, consistency, and appropriateness of AI's activities. This intentional deliberativeness will be messier than more autocratic societies, who don't have a plurality of different perspectives and view – yet we must proceed as such and show the world that the U.S. and other open nations can do this necessary work.

To rise to this challenge, we also must develop a new science of understanding the resiliency, and by extension the brittleness, of AI apps to disruption by false data, data poisonings, jailbreaking, and other exploits if both the public and the public service workforce is to trust interactions with AI. This is a role where the National Academy of Public Administration can help alongside multiple partners in developing such a science linked to public service, administration, and engagement.

Public Sector Leadership: Helping Communities Adapt to a New Era

By David Bray, PhD - Chair of the Accelerator & Distinguished Fellow, Stimson Center

Since its establishment in 1979, the Senior Executive Service (SES) has experienced a consistent set of pressures that impacts our nation's ability to respond to crises and disruptive events. A year-long study, using two decades of data sets from the Office of Personnel Management regarding long-term trends in the United States' government workforce, released its findings in 2019 noting:

1. A consistent pattern across *all* U.S. Presidential administrations: a steady increase in political SES appointments coupled with a decrease in non-political career executives. Notably: these shifts didn't occur under any one political party's rule.

1. A parallel trend where non-partisan SES members increasingly faced heightened scrutiny and criticism, including toxic controversies used as political leverage by opposing parties. This also has been a consistent trend since the 1990s onwards.

From these empirical results, the study authors concluded long-term trends, spanning at least two decades, had significantly diminished the capacity of public sector institutions to respond to a national crisis — or mount an adequate response if multiple domestic or foreign emergencies occurred at the same time. If workplaces continued to be politically charged, and if the relationships between elected and appointed political SES and non-partisan SES members continued to be toxic, this represented a recipe for seismic national disruption.

As such, the study warned in February 2019 that a national crisis-level event could happen in the next year where the U.S. government would not respond well to crisis because it no longer had the talent *and* it had made the workplaces so toxic that the connections and relations needed to respond wouldn't be there.

A year after that study, the COVID-19 pandemic happened. If the response proved suboptimal, it could be in part because of these overall workforce trends that have been growing over a period of at least two decades.

Yet we as a country can turn things around. Here is how:

Recognize the Need for Reform. Leaders from both sides of the political aisle, as well as from the private sector, must recognize that the United States needs a rejuvenation that begins by recognizing that renewed or *new* institutions are required to collaborate, coordinate, and adapt to new and emergent concerns quite differently than the world of 1979 when the Senior Executive Service was created. The post-World War II institutions of the past may not fit our interconnected world of 2025. Our institutions either need to be renewed or new, networked institutions that involve both public and private sector actors to be better prepared for future disruptions ahead.

Focus on Non-Partisan Solutions. The political environment for non-partisan senior executives in public service have become increasingly toxic over the last two decades. Online information that is either inaccurate or out of context can spread faster than the truth, adding to the already demanding work of non-partisan senior executives. To fix this, free societies around the world must strive to pull away from hyper-partisan politics and find value in bipartisan and non-partisan public service for the good of communities starting at local levels, then state levels, and finally nationally.

Foster Shared Public-Private Commitment. Free societies must re-awake shared community importance of a committed public and private sector ethos that supports a functioning set of governance activities for the economic, civic, and community health of towns, the 50 different states, and the nation, regardless of either individual or national politics or partisan media. It is only with functioning public and private sectors that free societies can be strong and resilient to disruptions.

There is no textbook for the future ahead – yet doing nothing is itself a risk of institutions becoming outdated, obsolete, and untrusted by a public that wants more from those who serve.

Onwards and upwards together.