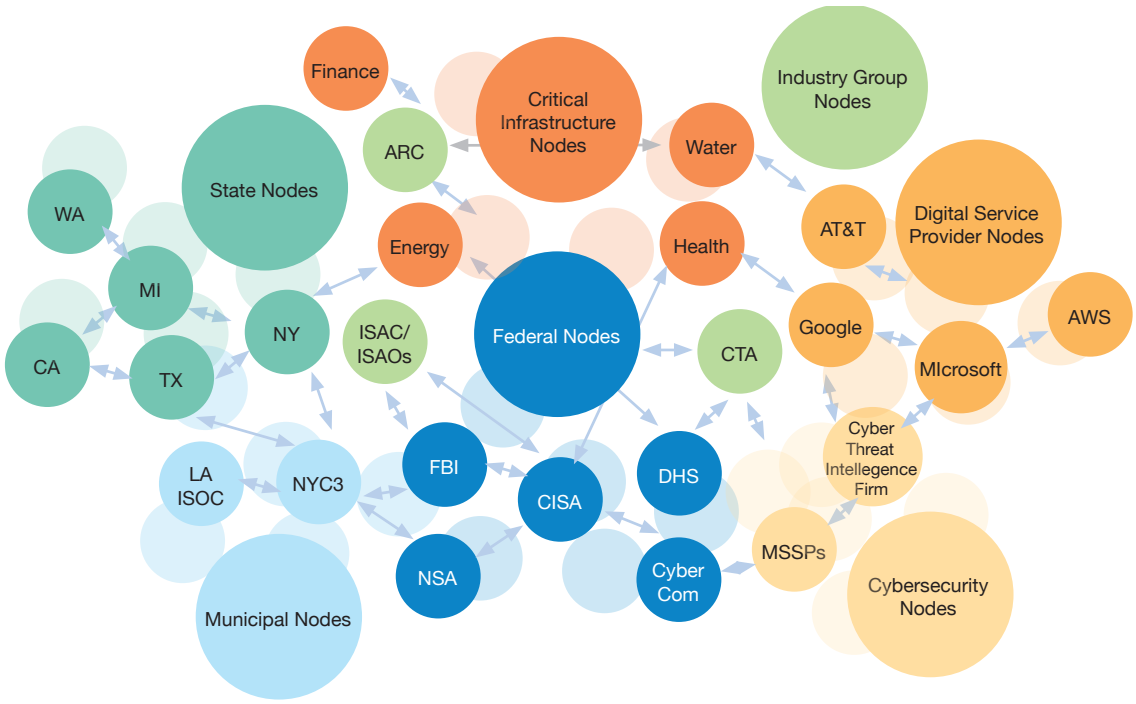
Enhancing Readiness for National Cyber Defense through Operational Collaboration

FINDINGS FROM THE NEW YORK CYBER TASK FORCE

The New York Cyber Task Force calls for a whole-of-nation effort by the public and private sector to enhance cyber defense readiness through operational collaboration. Geopolitical and social forces, growing technological dependencies, and inherent advantages for ever-more capable cyber attackers raise the risk of a major cyber crisis. Such a crisis could have significant adverse effects on public safety, the economy, and national security. Given mounting cyber challenges, the United States must take immediate steps to enhance its cyber readiness to withstand such potential attacks.

Columbia University's School of International and Public Affairs (SIPA) has sponsored the New York Cyber Task Force (NYCTF), a cross section of leading members of business, policy, and academia aiming to bring a unique perspective to key cyber policy issues. The NYCTF assessed future risks to U.S. national security stemming from cyber challenges including political, economic, and technological developments, changing cyber conflict dynamics, and, the COVID-19 pandemic. We envisioned severe, yet plausible scenarios projected for 2025 to examine how well the nation could defend itself in cyberspace. By looking to the future, the NYCTF has shifted away from yesterday's issues to focus on longer-term enhanced cyber readiness.

National Cyber Response Network



COLUMBIA | SIPA
School of International and Public Affairs

The New York Cyber Task Force, comprising of more than 45 leading experts from business, policy and academia, were gathered by Columbia University SIPA to analyze the degree to which the US was ready for future cyber adversaries. Co-Chaired by Greg Rattray (NextPeak), Dean Merit E. Janow (Columbia University SIPA), and Evan Wolff (Crowell & Moring)

The NYCTF recommendations seek to create an effective, whole-of-nation approach to enable enhanced cyber readiness through operational collaboration. At their core, these recommendations focus on establishing a public-private network of empowered nodes to provide effective crisis response to strategic cyber contingencies.

The NYCTF sees the development of this network as a fundamental step in enhancing cyber readiness. We also have identified key enabling conditions for enhanced cyber defense readiness. We hope to build on the momentum created by the recent Cyberspace Solarium Commission Report and the 2021 National Defense Authorization Act (NDAA), as well as actions taken at the state and municipal levels and by the private sector. The United States must undertake a focused, urgent cyber readiness effort through improving operational collaboration and can begin by implementing these recommendations.

Strengthening national cyber readiness should be seen as an opportunity, not as a burden. Cyber readiness in the face of severe but plausible cyber shocks will enable confidence in the digital transformations already underway. The campaign to defeat the coronavirus has taught us lessons about the need for resiliency, the need for collaboration across all levels of government and with the private sector, and the fundamental role trust plays in achieving such collaboration. The United States does not have to wait to learn these lessons over again if an adversary inflicts a severe cyber crisis upon us. The nation must get ready now.

Recommendation 1
Identify National Cyber Crisis Contingencies

Recommendation 2
Establish a National Cyber Response Network (NCRN)

Recommendation 3
Operation of the NCRN

Recommendation 4
Assess National Cyber Response Capabilities to Ensure Readiness

Recommendation 5
Ensure National Cyber Readiness through Training and Exercises

Enabling Recommendation 1
Establish Integrated Cyber Crisis Information Networks

Enabling Recommendation 2
Address Technology Evolution to Ensure Readiness

Enabling Recommendation 3
Remove Legal and Procedural Barriers to Enhance Response

Enabling Recommendation 4
Build Trust and Confidence for Cyber Crisis Response

Enabling Recommendation 5
Close Resource Gaps to Ensure Readiness

COLUMBIA | SIPA
School of International and Public Affairs