COLUMBIA
SIPA
School of International
and Public Affairs

BRIDGING THE TRUST GAP

FINDINGS FROM THE NEW YORK CYBER TASK FORCE

The New York Cyber Task Force (NYCTF) is a collaborative organization under the auspices of Columbia University's School of International and Public Affairs (SIPA) that brings together leading experts from academia, industry, and government agencies. The NYCTF's composition reflects its uniquely New York voice in the cybersecurity field. Its mission is to address cybersecurity challenges through research, education, and policy advocacy. The task force focuses on operational collaboration between the public and private sectors, conducting research to enhance cybersecurity practices, and providing guidance and recommendations to policymakers and organizations to make cyberspace more defensible.

The NYCTF has previously published two significant reports. The first, "Building a Defensible Cyberspace," was released in 2017. It provided recommendations aimed at strengthening the defense of cyberspace without compromising its utility and convenience. In 2021, the NYCTF released its second report, "Enhancing Readiness for National Cyber Defense through Operational Collaboration." This report presented a framework for operational collaboration based on a nodal model, using hypothetical future scenarios to identify ways of improving readiness.

This third report examines recent high-profile cyber incidents—SolarWinds, Colonial Pipeline, and Shields Up—to evaluate the private sector's perspective on operational collaboration. It uses these case studies to examine key gaps and identify points of leverage to improve how the government and industry work together. Over the past year, the NYCTF convened cybersecurity leaders and practitioners and conducted extensive interviews to investigate different perspectives on the case studies and the current and future state of operational collaboration. The task force report provides implementable policy recommendations to improve trust and operational collaboration between industry and government at scale. The report is organized around four key recommendations: improve US government crisis communications and transparency about cyber incidents; create professional incentives and opportunities for collaboration; establish a procedure for incorporating state and local stakeholders into operational collaboration; and establish a joint cyber warning center within the intelligence community.

Findings

The report identifies several key findings about operational collaboration that are common across all three cases, as well as those that are specific to the case studies.

In general, we found that:

- There has been significant progress in operational collaboration over the past decade.
- Challenges of trust in the government are enduring and multifaceted, lacking a whole-of-society approach. It is carefully cultivated over time, varies by context, and depends on grassroots, interpersonal, working relationships.
- The government faces challenges of effective crisis communication and coordination of messaging to the private sector.

- There is uncertainty within the private sector about how a growing regulatory footprint will affect operational collaboration.
- Effective operational collaboration often depends on size and maturity level, which is mismatched with the expectation that the government treats all companies equally.

Recommendations

The NYCTF report identifies four key recommendations, each buttressed by a number of supporting recommendations, to improve operational collaboration and trust. A core issue across the findings is that the US government typically has had three ways of interacting with the private sector: as a purchaser, regulator, or law enforcer. Yet none of these models is a good fit for operational collaboration. Therefore, our goal is to help define new ways of thinking about public-private collaboration beyond existing models.

Recommendation 1: Institutionalize crisis communications within the federal government. Multiple messages and communication channels from the government during an incident creates confusion and undermines credibility, trust, and effectiveness of response, especially when competing priorities are communicated.

Recommendation 2: Ensure that there are professional incentives and opportunities for collaboration within government and industry, and that the right people are in the room. People, expertise, and interpersonal relationships serve as the foundation for effective collaboration and the linchpin for cultivating trust.

Recommendation 3: Incorporate state and local stakeholders into operational collaboration. The federal government does not have the capacity to conduct incident response at scale for all state and local victims, and state and local governments vary significantly in cyber capability.

Recommendation 4: Establish a joint cyber warning center within the intelligence community that includes public and private sector elements. The warning should be clear about what the recipients of such information are expected or being asked to do as a response.