School of International and Public Affairs
Case Consortium @ Columbia
Columbia University

SIPA-21-0023.1

Operational Collaboration in Cyber Defense: A Columbia University Case Study

Executive Summary

As the essential functions of critical national infrastructure systems become reliant on digital technologies, securing those systems against cyber threats and ensuring their resiliency has become increasingly vital to national security in the United States and beyond. This new reality often puts private firms on the frontline of efforts to prevent, detect, thwart, and recover from cyber attacks. However, many experts in the cybersecurity and national security spheres warn that the proper systems and partnerships are not in place between local, tribal, state, and federal agencies and the private sector stakeholders with whom they need to communicate and coordinate before and during times of crisis. As such, there has been a recent push to formalize and deepen these public-private partnerships before an attack by criminals or nation-state adversaries compromise critical infrastructure sectors in a way that could lead to greater systemic harm to the economy, national defense, or public health.

This Columbia University case study explores the concept of "operational collaboration" and the argument for expanding both the breadth and depth of partnerships between the public and private sector in order to better protect critical infrastructure assets. In doing so, this case examines the systemic risks facing the U.S. government and private sector, the growing centrality of the private sector in defending the nation's critical infrastructure, some of the landmark achievements in industry-wide and public-private partnerships in cybersecurity, and the prospects for implementing operational collaboration under the Biden administration.

The case includes the following elements;

a) Video Intro and Discussions – Available Online

b) Written Case Study (This Document)

c) Annex A – Original Documents

Definition and Processes

This case was written by Sean Steinberg for the Picker Center Digital Education Group at Columbia's School of International and Public Affairs (SIPA). The faculty sponsors are Greg Rattray and Jason Healey.

In the context of cybersecurity, "operational collaboration" describes the various forms of proactive engagement that occur within "deep organizational partnerships" between relevant government bodies – such as intelligence agencies, national central banks, municipal transportation authorities, and militaries – and private firms – such as telecommunications operators, internet service providers, financial institutions, and energy providers – that "enable coordinated response to severely disruptive cyber crises."[1] prepare for, respond to, and recover from cyber attacks.

According to the co-chair of the 2020 New York Cyber Task Force, one of the pioneering forces in applying the concept to national cyber defense, operational collaboration is comprised of four distinct activities: *Joint Risk & Asset Identification, Warning of Emerging Threats, Contingency Planning,* and *Disruptive Operations*.[2]

Joint Risk & Asset Identification
This activity involves bringing together knowledgeable stakeholders from both the private and public sector actors to identify and weigh risks associated with computerized systems, digital networks, physical infrastructure, or the industry as-a-whole. Private firms specialized knowledge often positions them to be better acquainted with the technologies of their industry than a government actor operating from outside the sector, and therefore often makes private firms better suited to identify potential vulnerabilities and high-value targets. Once these risks have been identified and mapped, both parties can begin to prioritize in terms of defense and response. Cyber defenders from the public sector can also use this information to monitor for activities signaling an impending or ongoing cyber attack on the infrastructure.

Warning of Emerging Threats
This activity involves flagging stakeholders to impending or ongoing systemic cyber threats. Institutions of different sizes and capabilities are likely to have different visibility into these actions, with medium and smaller-sized organizations likely to have far less situational awareness. This can lead to "differing, uncoordinated responses." The NYCTF calls for a "common operating picture" among relevant actors, designed by a lead, central federal agency, comprised of "standing coordinated data flows, information processes, and communication and display tools." However, in the current climate, the government does not appear to have "adequate authority, processes, or tools to coordinate these actors."[3]

Contingency Planning
This activity involves bringing together relevant stakeholders to plan for "severe but plausible" cyber risk which might occur in order to assess readiness and identify capacity gaps. Similar activities are already utilized by federal agencies like the Department of Defense (DoD) and the Federal Emergency Management Agency to prepare for possible conflicts and natural disasters, respectively. The NYCTF's 2021 report on

[1] New York Cyber Task Force, Columbia University's School of International and Public Affairs. (2021). *Enhancing Readiness for National Cyber Defense through Operational Collaboration*. https://www.sipa.columbia.edu/ideas-lab/techpolicy/readiness-operational-collaboration.
[2] Stepan, A., & Rattray, G. (2021, April 20). Operational Collaboration Interview. personal.
[3] New York Cyber Task Force. *Enhancing Readiness for National Cyber Defense through Operational Collaboration*.

enhancing U.S. cyber-readiness calls for identifying potential crisis scenarios, as well as executing "shoulder-to-shoulder training, drills, and exercises" between public and private stakeholders.[4]

Disruptive Operations
This activity involves coordinating the resources and authorities of private and public entities to incapacitate the systems used to facilitate cyber attacks. As an example, when it comes to ransomware attacks, the Ransomware Task Force put forth a set of recommendations to disrupt the operations' profitability while increasing their risk for those executing them.[5] To do so, public-private partnerships can work to disrupt payment system and infrastructure used to facilitate the attacks and ransom payments, as well as disrupt the actors themselves through tactics like prosecution.

The most well-known recent example of recent joint disruptive operations were the disruption of the Trickbot botnet ahead of the 2020 U.S. Presidential election. Microsoft collaborated with international security firms as well as Financial Services Information Sharing and Analysis Center (FS-ISAC) identify and disable the IP addresses supporting the Trickbot's command-and-control center, under authorization provided by a U.S. district court. Around the same time, U.S. Cyber Command carried out its own, separate takedown operation against Trickbot.

Benefits of Operational Collaboration

Operational collaboration in cyberspace offers three key benefits: *Anticipation*, *Strategic Impact*, and *Operational Speed*. [6]

Anticipation:
Through daily coordination and intelligence analysis, operational collaboration can provide advanced transform a reactive cyber defense into a proactive one. By obtaining advanced warning of an attack, defenders can "preemptively align defenses against attack, as well as generate effective responses when attacks do occur."

Strategic Impact:
Operational collaboration allows stakeholders to focus energy and resources on their comparative advantages. For instance, telecommunication companies can analyze traffic on their networks to identify and filter malware; firms like Akamai can shut down Distributed-Denial-of-Service (DDoS) attacks; and web hosting providers like Microsoft can shut down IP addresses used to direct botnet attacks. Meanwhile, governments like the U.S, can take advantage of their more well-rounded intelligence to analyze adversaries' intentions and capabilities; they can provide a forum to train less sophisticated private sector entities that may become targeted and improve their cyber defenses; and they can use political and legal

[4] New York Cyber Task Force. *Enhancing Readiness for National Cyber Defense through Operational Collaboration*.
[5] Institute for Security and Technology. (2021). (rep.). *Combatting Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force*.
[6] Next Peak. (n.d.). Understanding Cyber Operational Collaboration [web log]. https://nextpeak.net/understanding-cyber-operational-collaboration/.

authorities to take aggressive and/or offensive actions such as "hacking back" at an adversary and compromising their cyber infrastructure within their own borders.

Inviting parties from both sectors to participate in strategic discussions can lead to a more integrated and inclusive defensive strategy. Rather than focusing on one-off tactics like "software patching, malware testing, server takedowns, [and] electronic seizures" which "only inflict temporary costs," partner organizations can "integrate resources to jointly plan and execute operations that maximize lasting disruption of adversary operations."

Operational Speed:
The cyber risk consulting firm Next Peak warns that "longstanding legal and policy restrictions currently limit freedom of action by government actors and stymie attempts to thwart attackers." This includes some regulations designed to protect privacy and preserve civil liberties, which in the digital age may have unintended consequences. For instance, because the National Security Agency (NSA) is not allowed to operate within the U.S., when it detects unusual computer traffic entering the country from outside it borders, it may have to "notify the FBI, which can then seek court permission and consult with the U.S. company that may be the target."[7] This process could give the attacker ample time to complete their activity and evade disruption.

Critical Infrastructure & Systemic Risk

Efforts to promote operational collaboration are closely tied to the "systemic risk" resulting from the Interdependencies of critical infrastructure sectors, such as banking, energy, telecommunications, transportation, and healthcare, which have been targeted by cyber criminals as well as nation-state level actors.

Today, much of this critical infrastructure – including payment systems, electrical grids, and even voter registration systems – rely on digital technologies, providing additional avenues for intrusion and disruption. 25 years after the Clinton administration's Commission on Critical Infrastructure, the federal government reinforced the gravity of risk facing these operations when the U.S. Department of Homeland Security (DHS) was instructed under Executive Order work with the sector specific agencies to identify "critical infrastructure" for which "a cyber incident would have far reaching impact on regional or national economic security."[8] One possible outcome of these systemic risks was foreshadowed in 2015, when Russian malware shut down the Ukrainian power grid in 2015 and caused billions in dollars of damages worldwide.[9]

Unfortunately, the "the evolving nature of cyber risk … is [still] not yet fully understood," according to the World Economic Forum, and "no ready-made curricula on systemic cyber risks and how to best

[7] Myre, G. (2021, April 6). *After A Major Hack, U.S. Looks To Fix A Cyber 'Blind Spot'*. NPR. https://www.npr.org/2021/04/06/983872116/after-a-major-hack-u-s-looks-to-fix-a-cyber-blind-spot.

[8] Exec. Order No. 13,636, 3 C.F.R. (2014)

[9] Greenberg, A. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *WIRED*. Aug. 22, 2018.

manage them exist."[10] Contributing to this problem, the U.S. to this day still relies on a "patchwork of organizations" for its various cyber defense needs, according to the NYCTF, rather than the "integrated response network required to deal with … sophisticated cyber attack[s]." The Task Force also identifies the imbalanced amount of attention paid to the federal government when it comes to tackling systemic cyber risk, advocating instead for a "whole-of-nation perspectives" more inclusive of state and local government leaders.[11]

The New Frontline Goes Through the Private Sector

While these issues hold severe implications for national security, the cyber domain offers unique challenges in that many of the assets being targeted reside in the private sector, as does the capacity and technology to protect them. The Cyberspace Solarium Commission (CSC) – a Congressionally-authorized investigatory body designed to propose improvements to American cyber defense strategy - itself concluded that "government is often not the primary actor" in cyberspace.[12]

In the United States, many firms supporting the nation's critical infrastructure are private entities, "the majority of operational assets and capabilities to provide digitally enabled services are owned and operated by the private sector," and the private sector arguably houses the foremost subject-matter expertise on cybersecurity. Compounded by the growth of novel technologies like cloud computing, Internet of Things (IoT), and artificial intelligence (AI), as well as the increasing prevalence of big data and machine learning,[13] the "convergence of information technology (IT) and operational technology (OT), and the expansion of internet-connected people, places and things creates an expanded attack surface" that can be exploited by adversaries.[14]

However, critics of past and current U.S. defensive efforts in the cyber domain contend that public and private stakeholders remain too siloed, complaining of "a lack of coordinated policies and regulations" not only between public and private sector stakeholders, but also between private cybersecurity firms and the private industries comprising critical infrastructure. This siloed model may be partially responsible for a major "blind spot" into "the evolving nature of cyber risk," as cyber risk assessments conducted by private firms are often internally focused, and their findings are often inaccessible to outside actors who may share their risk either due to sharing their vulnerabilities or their unseen digital ties to the organization in question, as demonstrated in the SolarWinds attack. [15]

---

[10] World Economic Forum. (2016). (rep.). *Understanding Systemic Cyber Risk*.

[11] New York Cyber Task Force. *Enhancing Readiness for National Cyber Defense through Operational Collaboration*.

[12] U.S. Cyberspace Solarium Commission. 2020. 2 Mar. 2021. https://www.solarium.gov/report.

[13] World Economic Forum. *Understanding Systemic Cyber Risk*.

[14] Ciampoli, P., & Harrell, B. (n.d.). Protecting critical energy infrastructure: Q&A with CISA's Harrell. other. https://www.publicpower.org/periodical/article/protecting-critical-energy-infrastructure-qa-with-cisas-harrell.

[15] World Economic Forum. *Understanding Systemic Cyber Risk*.

Meanwhile, U.S. government agencies until recently often were positioned as the lead figure in the national cyber defense, rather than acknowledging the private sector's advantages in securing its own networks. This mindset was epitomized by the "collect it all" approach to data the National Security Agency's (NSA) adopted under the leadership of General Keith Alexander. Alexander had alarmed financial industry officials in the early 2010s when he allegedly proposed that "private companies … give the government access to their networks so it could screen out the harmful software," an offer which they feared would represent "unprecedented intrusion" into their private databases.[16] However it is not clear that such an expansive data collection effort would have even been effective had it been operationalized, given the overwhelming amount of data the agency would have assumed responsibility for which was previously controlled by multiple, separate multinational institutions.

This philosophy may be on its way out, however, insofar as the CSC's 2020 report recognizes that "private-sector entities have primary responsibility for the defense and security of their networks." This report also validates the need to "operationalize cybersecurity collaboration with the private sector" as one of its six key pillars. Noting the vital role played by cloud platforms, IoT, and AI play in today's economy and critical infrastructure - particularly in the areas of finance, e-commerce, manufacturing, and healthcare.[17] NYCTF recommends that technology sub-sectors be integrated into its multi-sector "National Cyber Response Network" along with other critical infrastructure and government partners.[18]

Beyond Info Sharing

Those who favor operational collaboration critique the prevalent public-private cyber defense model for relying exclusively on information sharing activities, as opposed to their more holistic approach which also includes activities like joint intelligence warning regarding systemic threats, contingency planning, or the cooperative disruption of adversaries.

This tendency towards information sharing as a primary activity for public-private collaboration in cyberspace could be seen in the establishment of the private-sector FS-ISAC in 1999, although it is not the only organization designed specifically to share cyber threat information. While some even crossed the public-private divide, none "nourished the level of operational information sharing required for public-private response at a scale to effectively coordinate response during a major cyber crisis," according to NYCTF. [19] Barriers to information sharing exist even within government itself, and sometimes even within the same bureau, as when the Cybersecurity and Infrastructure Security Agency (CISA) rejected requests from its DHS headquarters for proprietary information related to SolarWinds provided by private-sector partner. This resistance, it appears, was due both to fears that the request was driven by the

[16] Washington Post: https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html
[17] U.S. Cyberspace Solarium Commission. 2020. 2 Mar. 2021. https://www.solarium.gov/report.

[18] New York Cyber Task Force. *Enhancing Readiness for National Cyber Defense through Operational Collaboration*.

[19] New York Cyber Task Force. *Enhancing Readiness for National Cyber Defense through Operational Collaboration*.

administration's political considerations, and to avoid betraying the confidential agreements in place with its private-sector partners.[20]

Some possible impediments to effective info-sharing are existing legal and policy barriers in both sectors, argues NYCTF, making their removal a key objective of the task force. From the private side, firms fear incurring liability for sharing information regarding vulnerabilities, while national security concerns have bred reluctance among government agencies to share intelligence with private actors. The U.S. Senate passed the Cybersecurity Information Sharing Act in 2015 to alleviate these concerns by providing legal immunity to companies sharing information about cyber threats, vulnerabilities, defensive measures, and damages with the government, and in return mandating greater sharing of both classified and unclassified information by U.S. intelligence. However, the NYCTF still believes there is more to be done to lower these barriers. It proposes granting "proper authority to exchange necessary and appropriate information," (a step which involves clarifying and assuaging reputational/business/liability concerns), ensuring municipal- and state-level governments have access to federal intelligence, avoiding overregulation of cyber-related issues, and incentivizing greater investment in resiliency measures.[21]

Nonetheless, information sharing remains an important part of operational collaboration, even if the activity cannot by itself "provide the joint response capabilities necessary to warn of, and mitigate and recover from systemic cyber attacks." The CSC, for example, recommends developing a cloud-based platform which would make "the federal government's unclassified and classified cyber threat information, malware forensics, and network data from monitoring programs … commonly available for query and analysis" for the private sector, and vice-versa.

Bridging the Divide

Recent years have seen a growing number of institutions embracing cross-sector approaches to cyber defense, and the Biden administration's own defense priorities reflect a growing integration of the private sector into the national cyber defense.

CEOs of eight systemically important American bank took the initiative to launch the Financial Systemic Analysis and Resilience Center (FSARC), originally an FS-ISAC subsidiary which aims to facilitate collaboration withing the industry and beyond to the public sector. Its public-sector partners include federal U.S. agencies like the Treasury, DHS, the intelligence community and the Federal Bureau of Investigations (FBI), and its activities thus far have been beneficial for systemic threat analysis, warning and contingency planning. With input from its membership and other financial sector organizations, FSARC developed a confidential "risk register" – a list of "business processes, functions, and technologies underpinning the U.S. financial sector which, if compromised, could lead to systemic risk" – and also developed a list of "nearly two dozen cyber scenarios" that could cascade from one institution into the entire sector.[22] The FSARC has made its risk register available not only to its members, but also other financial sector organizations and its government partners.

[20] https://www.politico.com/news/2021/01/05/dhs-cisa-company-data-solarwinds-455229

[21] New York Cyber Task Force.

[22] Financial Systemic Analysis & Resilience Center. "U.S. Treasuries (UST) Initiative Highlights." https://www.newyorkfed.org/medialibrary/Microsites/tmpg/files/FSARC_TMPG_Presentation.pdf.

After the financial sector got the ball rolling, we've seen growing efforts to bring additional sectors into similar working groups. DHS has brought together senior industry and government representatives from the financial and communications sectors, the electricity sub-sector, DHS, the Treasury, and the Department of Energy for its Tri-Sector Executive Working Group. The Analysis and Resilience Center for Systemic Risk in 2020 brough together leaders from energy and finance to collaborate on analysis, threat monitoring, and the development of "resilience measures" with government partners.[23]

Even organizations originally designed specifically to engage in information-sharing like FS-ISAC have recognized the need to evolve the parameters of their partnerships. Today, FS-ISAC says that it also engages in contingency planning exercises, education and training programs, and rapid response communication management "with and among other key sectors and government agencies." In addition to coordinating sector-wide responses to malware, worm, and DDoS attacks (including the 2012 Iranian attacks on the financial sector), it also sought to protect consumer confidence in the event of widespread compromise of banking data by offering a "guide [to] deposit insurance in the event of" the cyber-induced collapse of a financial institution. The lessons gleaned for this guide were reportedly "a direct result of lessons learned from cyber exercises."[24]

Perhaps one of the most significant benchmarks for government-led progress can be seen in the 2021 National Defense Authorization Act (NDAA). Of the 26 CSC recommendations adopted into the NDAA, at least eight appear relevant to increasing operational collaboration (see: Annex A-1). Recommendations from the CSC include regular cross-sector cyber training exercises, joint planning offices for cybersecurity campaigns, codification of risk management agencies relevant to critical infrastructure, and assessment of ongoing and previous public-private cybersecurity collaboration.

Although U.S. cyber defenses successfully helped preserve the integrity of the 2020 Presidential Election through individual operations like the Trickbot takedown, the election subsector still lacks the deep, institutionalized public-private partnerships called for in this case study, and both sectors seem to remain siloed in separate working groups. The Election Infrastructure Subsector Government Coordinating Council (GCC) hosts federal, state, and local government stakeholders, while election industry is represented by the Election Infrastructure Subsector Coordinating Council (SCC). One of the few examples of cross-sector efforts noted by a 2020 CISA report was when the SCC sent a single representative in 2018 to serve on a Critical Infrastructure Cross-Sector Council working group which aims to "educate all sectors about the causes and effects of long-term power outages and the importance of developing cross-sector recommendations."[25]

Recent high-profile breaches of corporate tech giants, private cybersecurity leaders, and highly-sensitive government servers may offer further opportunities to illustrate the stakes of neglecting effective

[23] Announcing the Formation of the Analysis & Resilience Center (ARC) for Systemic Risk. (2020, October 30). *Street Insider*.

[24] Healey, J., Mosser, P., Rosen, K., & Tache, A. (2018). (rep.). *The future of financial stability and cyber risk*. Washington, DC: Brookings Institution.

[25] U.S. Cybersecurity and Infrastructure Security Agency. (2020). *Election Infrastructure Subsector-Specific Plan: An Annex to the NIPP 2013*.

partnerships. The SolarWinds attack - which breached private firms as well as sensitive federal government systems belonging to the DoD, DHS, and Department of Justice, among other agencies. Cyber Command head General Paul Nakasone testified to a Senate committee that cyber defense agencies require more leniency to respond quickly to attacks, stating current authorities prevented Cyber Command and the NSA from having the agility needed to defend against adversaries operating out of infrastructure located within U.S. borders.[26] Additionally, former NSA general counsel Glen Gerstell proposed creating a "fusion center" that would combine the resources of the FBI, NSA, and CISA with those of the private sector. Nakasone's testimony, however, received a mixed response in the Senate: while several senators seemed ready to offer the agency new privileges, one privacy-minded politician spoke out critically, concerned over the possibility of "warrantless surveillance of Americans' communication" following the exposure of the NSA's illegal domestic surveillance operations during the previous decade.[27] However, at least one positive concrete achievement did come out of these incidents in the form of a joint working group by DHS, NSA, the Office of the Director of National Intelligence, and unnamed private sector organizations in response the disclosure of security issues related to MS-Exchange.[28]

Conclusion

In the nearly three decades since an American president first sought to understand the cyber risks associated with the nation's critical infrastructure, the country's private and public sectors have conducted much of their cyber defensive efforts in relative isolation. When contact was made, the relationship often began and ended with the sharing of threat information. But with American private firms today more often being made the vector of cyber attacks by politically-minded geopolitical adversaries and technologically sophisticated criminals, these partnerships need to be made more communicative, collaborative, and must cover a wider range of activities. These activities should cover all aspects of cyber defense, including risk identification, cross-sector training exercises, joint responses, and resiliency and recovery planning. So far, the progress of the Biden administration has taken steps which suggest expanding public-private partnerships in the cyber domain may be on their way. But until those partnerships more fully materialize and produce actionable results, the progress largely exists on paper.

---

[26] Tucker, P. (2021, April 14). *Senators Offer to Let NSA Hunt Cyber Actors Inside the US*. Defense One. https://www.defenseone.com/technology/2021/03/senators-offer-let-nsa-hunt-cyber-actors-inside-us/172938/.

[27] Myre, G. (2021, April 6). *After A Major Hack, U.S. Looks To Fix A Cyber 'Blind Spot.*

[28] Johnson, D. F. B. (2021, March 18). *White House forms public-private task force to tackle Microsoft hack*. SC Magazine. https://www.scmagazine.com/home/security-news/vulnerabilities/white-house-forms-public-private-task-force-to-tackle-microsoft-exchange-hack/.

ANNEX A: Original Documents

Annex A-1: Relevant provisions (National Defense Authorization Act of 2021)

Annex A-2: Visualization: National Crisis Response Network ("Enhancing Readiness for National Cyber Defense through Operational Collaboration")

Annex A-3: Visualization: National Crisis Response Network Operational Concept ("Enhancing Readiness for National Cyber Defense through Operational Collaboration")

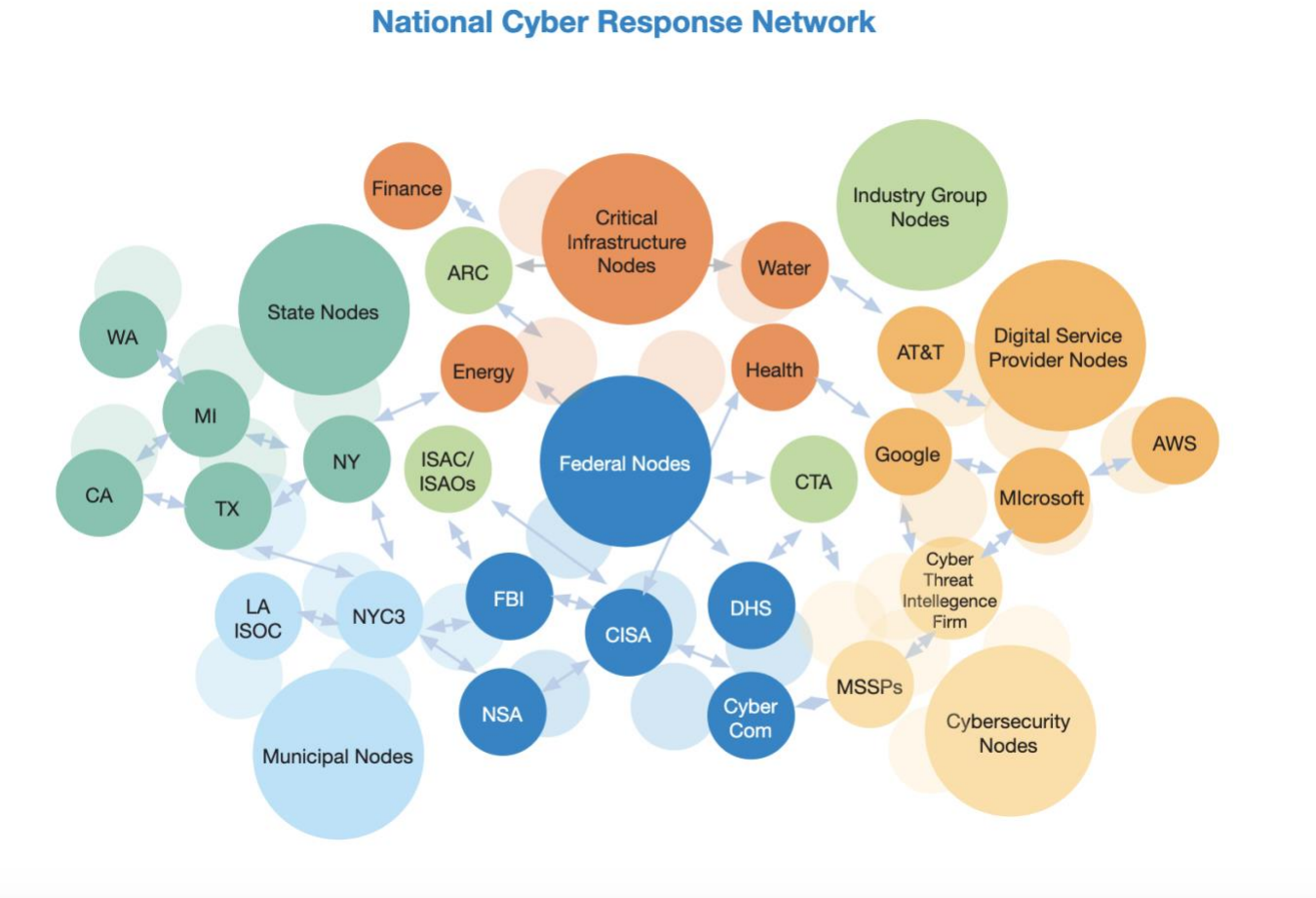
Annex A-1

Recommendations of the Cyberspace Solarium Commission listed as provisions for the National Defense Authorization Act of 2021 (as relevant to operational collaboration).

1. Establishment in DHS of the Joint Cyber Planning Office
    a. Establishes a Joint Cyber Planning Office under CISA, to facilitate comprehensive planning of defensive cybersecurity campaigns across federal departments and agencies and the private sector.
2. Cybersecurity Advisory Committee
    a. Establishes a Cybersecurity Advisory Committee to advise DHS/CISA.
3. Administrative Subpoena Authority for the Cybersecurity and Infrastructure Security Agency
    a. Grants administrative subpoena authority to CISA in order to identify vulnerable systems and notify public and private system owners.
4. Codify Sector Risk Management Agencies
    a. Codifies Sector Specific Agencies as Sector Risk Management Agencies, establishing minimum responsibilities and requirements for identifying, assessing, and assisting in managing risk for the critical infrastructure sectors under their purview.
5. Creation of a Biennial National Cyber Exercise
    a. Establishes a federal government cyber exercise to be conducted every two years for ten years to include federal, state, and private sector stakeholders, as well as international partners.
6. Assessing Private-Public Collaboration in Cybersecurity
    a. Requires the Department of Defense to assess of the impact of the current Pathfinder initiative, the Department's support to and integration with existing Federal cybersecurity centers, and comparable initiatives led by other Federal departments or agencies that support long-term public-private cybersecurity collaboration and make recommendations for improvements.
7. Defense Industrial Base Participation in a Threat Intelligence Sharing Program
    a. Requires the Department of Defense to assess the feasibility, suitability, and definition of, and resourcing required to establish a defense industrial base threat information sharing program.
8. Defense Industrial Base Cybersecurity Threat Hunting and Sensing, Discovery, and Mitigation
    a. Requires the Department of Defense to complete an assessment of the feasibility, suitability, and resourcing required to establish a defense industrial base cybersecurity threat hunting program.

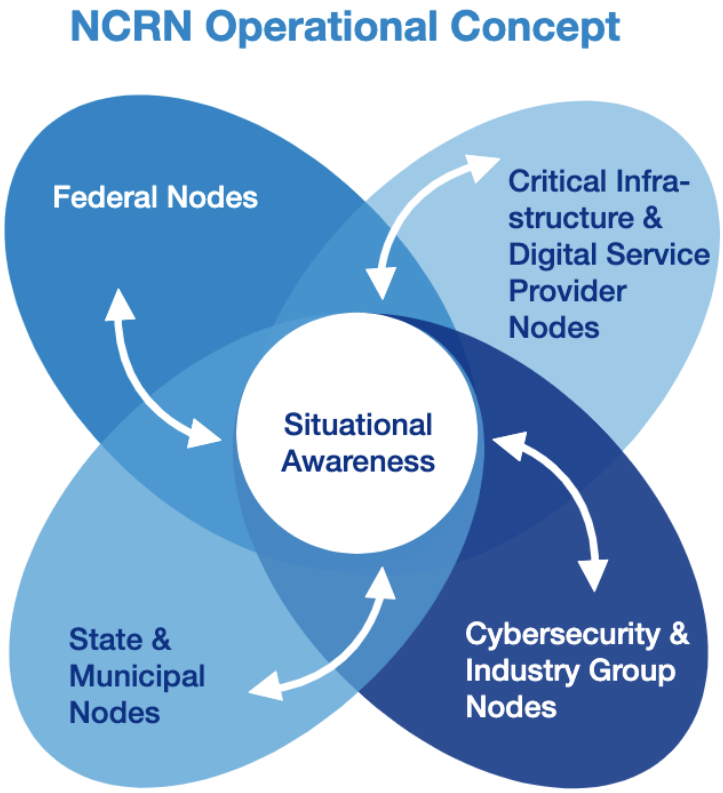
Annex A-2

Visualization: "National Crisis Response Network" (drawn from the New York Cyber Task Force's 2021 publication, "Enhancing Readiness for National Cyber Defense through Operational Collaboration"



Annex A-3

Visualization: "National Crisis Response Network Operational Concept" (drawn from the New York Cyber Task Force's 2021 publication, "Enhancing Readiness for National Cyber Defense through Operational Collaboration"



Nodes feed:
- Attacks and Impacts
- Responder Status
- Current Actions
- Missions
- Objectives
- Desired State & Communications

Nodes receive:
- Intelligence
- Common Operating Picture
- Cyber Defense Actions
- Planned Proactive Defense Measures
- Desired State & Communications