ASPEN CYBERSECURITY GROUP

THE ASPEN INSTITUTE

# An Operational Collaboration Framework for Cybersecurity

November 2018

## About the Aspen Cybersecurity Group

The Aspen Cybersecurity Group is a cross-sector public-private forum comprised of former government officials, Capitol Hill leaders, industry executives, and respected voices from academia, journalism, and civil society that have come together to translate pressing cybersecurity conversations into action. At its inaugural meeting in January 2018, the group decided to focus its efforts in three key areas of need as requiring urgent attention by a group that crosses party lines and includes both policymakers and practitioners: (1) improving operational collaboration between the public and private sector; (2) developing the skills and education necessary for a workforce that will increasingly confront cybersecurity challenges; and (3) securing and ensuring confidence in emerging technologies, including the Internet of Things (IoT).

*Co-Chairs:*

**U.S. Representative Will Hurd** (TX-23)
**Lisa Monaco** (Distinguished Senior Fellow, NYU Law School, Center on Law and Security, and Center for Cybersecurity)
**Ginni Rometty** (Chairman, President, and CEO, IBM)

*Members:*

**John Carlin** (Chair, Cyber & Tech Program, Aspen Institute)
**Keith Alexander** (President and CEO, IronNet Cybersecurity)
**Sara Andrews** (CISO, Pepsi)
**Monika Bickert** (Head of Product Policy and Counterterrorism, Facebook)
**Vint Cerf** (Chief Internet Evangelist, Google)
**Greg Clark** (CEO, Symantec)
**Dr. Lorrie Faith Cranor** (Professor, Carnegie Mellon University)
**Michael Daniel** (President and CEO, Cyber Threat Alliance)
**Jim Dempsey** (Executive Director, Berkley Center for Law & Technology)
**Don Dixon** (Co-Founder & Managing Director, Trident Capital Cybersecurity)
**Lynn Good** (CEO, Duke Energy)
**Alex Gorsky** (CEO, Johnson & Johnson)
**Yasmin Green** (Director, Research & Development, Jigsaw)
**Michael Hayden** (Principal, The Chertoff Group)
**Susan Hennessey** (Managing Editor, *Lawfare*)
**Chris Inglis** (U.S. Naval Academy)
**Sean Joyce** (Partner, PwC)
**Dr. Herb Lin** (Senior Research Scholar & Research Fellow, Stanford University)
**Brad Maiorino** (Executive Vice President, Booz Allen Hamilton)
**Chandra McMahon** (Senior Vice President & CISO, Verizon)
**Dr. Gregory Rattray** (Director of Global Cyber Partnerships, JPMorganChase)
**Former Rep. Mike Rogers** (Distinguished Fellow & Trustee, Center for the Study of the Presidency and Congress)
**David Sanger** (National Security Correspondent, *New York Times*)
**U.S. Representative Adam Schiff** (CA-28)
**Dr. Phyllis Schneck** (Managing Director, Global Leader of Cyber Solutions, Promontory Financial Group, an IBM Company)
**Alex Stamos** (Adjunct Professor, Stanford University)
**Dr. Hugh Thompson** (CTO, Symantec)
**Kathy Warden** (President and COO, Northrop Grumman)
**Michelle Zatlyn** (COO and Co-Founder, Cloudflare)
**Jonathan Zittrain** (Director, Harvard Berkman-Klein Center for Internet & Society)
***Jane Harman*** *(ex-officio)*
***Michael Chertoff*** *(ex-officio)*

# An Operational Collaboration Framework for Cybersecurity

**To reduce the risk of cyber threats and the impact of cyber incidents, as a society we must bring to bear capabilities resident in many different organizations in the public and private sectors.** Operational collaboration—bringing together a full spectrum of operational capabilities and authorities in persistent proactive efforts to counter cyber threats—needs to occur in both a "Steady State" environment and during significant cyber incidents as defined by the National Cyber Incident Response Plan (NCIRP)[1]. In the Cyber Incident Severity Schema of the NCIRP, it is not until Level 2 where active operational collaboration would begin to take place. Effective operational collaboration in a "Steady State" environment may reduce the number of significant cyber incidents requiring a response.

**However, the concept of operational collaboration in a cybersecurity environment is not well understood.** Some factors that prevent relevant public and private sector actors from conducting effective operational collaboration are:

- No defined framework for organizing operational collaboration
- Lack of clarity regarding the relevant players
- Unclear roles and responsibilities of those players
- Undervaluing proactive operational cooperation between the public and private sectors

This paper explores how the U.S. government and its private sector partners could address these problems and create an effective framework for cybersecurity operational collaboration. The intent is to enhance existing processes and relationships in order to facilitate a more efficient and effective model.

## Framework Defined

**Operational collaboration should occur in five mission areas: Protect, Mitigate, Prevent, Respond and Recover.** This cyber collaboration framework is similar to the National Preparedness System which is used to coordinate responses to natural disasters, terrorism, chemical and biological events in the physical world. As the linkage between the cyber and physical realms increases, using similar organizing constructs for both environments would make coordination between the two realms more seamless.

- *Steady state*: The Protect, Mitigate, and Prevent missions comprise the collaboration areas in a "steady state" environment or the normal operating state of the world.[2]

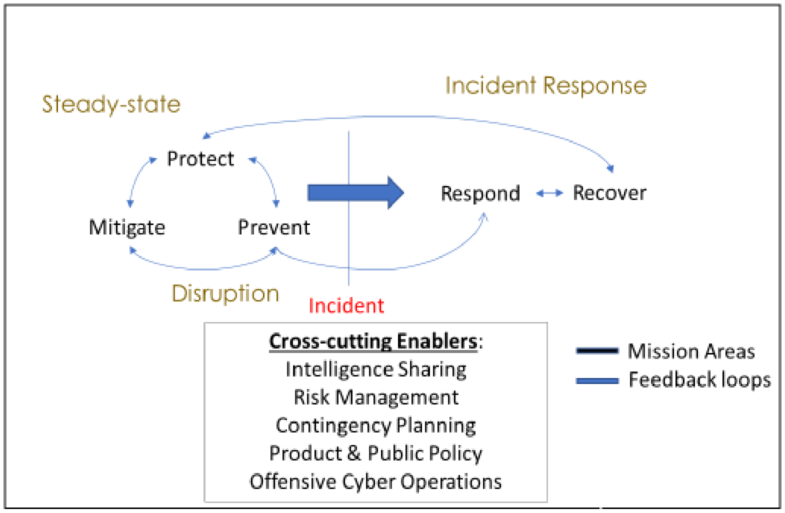
[1] National Cyber Incident Response Plan. Found at https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[2] In the preparedness framework, the prevent mission area focuses on actions taken against adversaries; therefore, proactive disruption efforts, such as a botnet takedown, would fall under

- *Incident Response*: When a cyber incident occurs that has a broad impact on our digital ecosystem (whether from a national security, economic, or public health and safety point of view), then the action shifts to the Response and Recovery missions.

Feedback loops should exist between all the mission areas, with the lessons learned in one mission informing the actions in another. The diagram below depicts how these missions fit together.

Framework for Operational Collaboration



**Cross-cutting Enablers**:
Intelligence Sharing
Risk Management
Contingency Planning
Product & Public Policy
Offensive Cyber Operations

**Protect and Mitigate**

Relevant actors collaborate to raise the level of cybersecurity across the digital ecosystem and to mitigate the potential impact of cyber threats. Key activities include risk management to identify critical systems and lower risk appropriately, addressing vulnerabilities, developing and sharing information and intelligence on emerging threats, developing a deep understanding of threats and the ability to warn of attacks, implementing cybersecurity best practices, conducting research on interdependencies, establishing contingency plans, and conducting exercises.

**Prevent**

Relevant actors synchronize actions to disrupt the activities of malicious cyber actors prior to and outside of a response to a specific incident. Key activities include exposing malicious cyber

the "Prevent" phase. What cybersecurity professionals typically call prevention activities (e.g., setting a firewall rule to prevent an intruder from gaining access) would fall under the protect or mitigate mission areas under this framework.

campaigns publicly, botnet take-downs, law enforcement actions against companies, economic sanctions, and other cyber and non-cyber government counter measures against malicious cyber actors.  Private sector actors will only operate on their own networks; government actors may conduct offensive cyber operations on other networks to prevent and deter attacks, when appropriate.

### Respond and Recover

The relevant actors are responding to and/or recovering from an incident that is either on-going or has already occurred.  Progress has been made in this mission area, including improved information sharing to ensure that adversary tactics, techniques, and procedures have a limited effective lifespan and the development of plans and policies such as the National Cyber Strategy, Presidential Policy Directive 41 and the National Cyber Incident Response Plan.  Key activities include rapidly identifying the incident's underlying cause, sharing and implementing effective defensive measures to contain or prevent further damage, and synchronizing specific response actions, such as dropping packets or re-routing traffic.

## Cross-cutting enablers

Under this framework, effective operational collaboration in these mission areas depends on five cross-cutting enablers. These enablers can be in place without operational collaboration occurring, but collaboration will only succeed if these enablers are functioning well.

### Intelligence and Information Sharing

The relevant actors in the private and public sectors need to engage in the sharing of information and intelligence to understand threats and inform defensive efforts, law enforcement activity, and other counter measures as appropriate. Current efforts that encourage cross-sector sharing and collaboration are positive and worthy of support. Specific activities related to intelligence collaboration include:

- Technical data – observables, indicators of compromise (IOC), and tactics, techniques, and procedures (TTP)
- Context – why is an IOC malicious or how a TTP is used
- Attribution – who is behind a particular set of malicious actions
- Best practices – useful actions to better secure IT networks in general
- Defensive measures and mitigations – specific actions to thwart adversary activities
- Strategic warning – general warning about adversary activity
- Tactical warning -- specific warning given to a particular entity
- Situational awareness – what's happening right now

### Risk Management

Without effective risk management, organizations will not be sufficiently protected against cyber threats. Therefore, all organizations should use a risk management framework for their cybersecurity activities. The NIST Cybersecurity Framework is a critical tool for guiding risk management activities within the Protect and Mitigate mission areas. As a part of risk management, organizations must be able to identify their most critical systems and analyze the risk to their operations and any cross-sector impacts.  Precise understanding of risk in key critical infrastructure systems requires a joint effort between the owners and operators of the infrastructure, USG Sector Specific Agencies, national laboratories, and others.

### Contingency Planning

Effective planning is important within every mission area.  Under this framework, the government and the private sector should jointly develop contingency plans for using different capabilities.  Existing exercises, like Cyber Storm and Quantum Dawn, should be incorporated into this enabler.

### Offensive Cyber Operations

These types of operations take place on networks belonging to other organizations or countries than the actor.  Only governments have the authority to carry out such activities.  These actions can be carried out both in the prevention and response mission areas.  The government may choose to involve certain elements in the private sector in order to enhance the effectiveness of offensive actions, but private sector companies would not carry out offensive actions. Effective conduct of offensive cyber operations also may contribute to the deterrence of cyber-attacks.

### Product and Public Policy

Product and public policy should enable actors to engage in effective collaboration in each of these mission areas.  The appropriate organizations and investments must also occur to ensure that joint operational collaboration activities can occur in a well synchronized and materially effective fashion.

## Relevant actors

**Effective operational collaboration is resource intensive and is not a commodity tool**. To implement a collaboration framework like the one described above, the right organizations need to be identified, specific people within those organizations tagged with the responsibility of carrying these missions, and the right structures need to be in place for these organizations to interact, during both steady state and incident response. For cybersecurity, this step is complicated because many relevant actors are private sector entities and the number of actors could be very large. If the collaboration includes too few actors, it won't be effective; however, if it includes too many, it will become unwieldy.

Therefore, as a starting point, we should focus operational collaboration in the private sector on those entities that are best positioned to take cybersecurity actions on behalf of the largest possible constituency; have access to cybersecurity information and intelligence that can be used for protection and can be shared broadly; or have high-level national or economic security relevance and are positioned to contribute to cybersecurity on a systemic basis (i.e. beyond a single company). In this manner, we can use leverage to address cybersecurity threats and incidents in a scalable way, where these companies take action on behalf of their customers and partners.

- An National Security Telecommunications Advisory Committee report[3] lays out the foundation for such an identification; that report recommended that the essential principle be whether the entity can take cybersecurity actions affecting more than itself. These actions could include, for example, cybersecurity companies providing specific cybersecurity protections into products that their customers use, or internet service providers diverting known malicious traffic away from its customers. In addition, the entity should be able to take action at a measurable scale and relatively quickly (within hours or days)

Starting with these principles, **five categories of private sector entities are the most likely relevant actors for operational collaboration:**

- cybersecurity providers;
- telecommunications and Internet Service Providers (ISPs);
- information technology companies (hardware, software, and service providers
- systemically important critical infrastructure sector companies; and
- information sharing organizations that have developed particular cybersecurity capabilities and information sources.

At present, the number of U.S. companies and organizations who meet these criteria is unknown; further research and market analysis is needed to identify these entities. Further, not all potentially relevant actors will need to participate in every aspect of operational

[3] The President's National Security Telecommunications Advisory Committee. *NSTAC Report to the President on Information and Communications Technology Mobilization.* 2014. Found at: https://www.dhs.gov/sites/default/files/publications/NSTAC%20-%20Information%20and%20Communications%20Technology%20Mobilization%20Report%2011-19-2014.pdf.

collaboration all the time. Therefore, we need the flexibility to expand or contract collaboration groups depending on the specific situation.

Finally, private sector actors change over time. Companies go out of business, merge or close; new companies emerge. The government also wants to encourage competition and does not want to create barriers to entry in the cybersecurity or telecommunications market, or preferentially benefit some organizations based on personal relationships. Therefore, the framework needs to accommodate these shifts in the private sector. As a result, identification should be criteria based – if the organization meets the criteria and will agree to the operating principles used in the collaboration process (such as honoring information embargoes), then it can and should participate.

For the public sector, relevant policies spanning several administrations have identified the key departments and agencies with cybersecurity missions. Specifically, for incident response collaboration, Presidential Policy Directive-41[4] lays out the roles and responsibilities for departments and agencies. PPD-41 identified three lines of effort for the Federal government in cyber incident response and a lead agency for each: threat response – FBI, asset response – DHS, and intelligence support – Office of the DNI. PPD-41 also lays out the coordination mechanisms the Federal government will use in responding to a significant cyber incident. The collaboration process in the response mission area should build upon this existing structure and support the objectives described in the September 2018 National Cyber Strategy for public-private collaboration to defend critical infrastructure.

### Roles and Responsibilities

Once the relevant actors have been identified, they need to know the roles and responsibilities of the other relevant actors. For a private sector entity, its roles and responsibilities should be driven by a combination of its products, services, capabilities and span of networks that it controls. For the U.S. government, roles and responsibilities can differ, depending on the mission area.

### Next Steps

This paper lays out a framework for conceptualizing how operational collaboration could work in the U.S. context. However, to make this framework a reality, both the public and private sectors need to take additional actions. Therefore, the Aspen Cybersecurity Group recommends that the U.S. government and relevant private sector entities:

1. **Agree on the criteria for participation** – as noted above, we need criteria for which entities to try to proactively include in the collaboration process. We should use a

[4] Presidential Policy Directive/PPD-41. *Presidential Policy Directive – United States Cyber Incident Coordination.* 2016. Found at: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

multi-stakeholder approach, like the process used for reaching consensus in Internet Governance issues, to develop these criteria.

2. **Identify the relevant private sector organizations in each category** – although the number could be large, it is not infinite. Therefore, we should use the same multi-stakeholder process to achieve consensus regarding the relevant participants in each category.

3. **Agree on roles and responsibilities** – once the relevant actors have been identified, we should agree on the roles and responsibilities each actor will take on in this area. Draft roles and responsibilities are included with this report in table 1 below.

4. **State actions to support mission areas and cross-cutting enablers** – table 2 provides a summary of specific actions the public and private sectors could take to implement the operational collaboration framework.

## Table 1: Typical Roles and Responsibilities

| Type of Actor | Responsibility | Actions |
|---|---|---|
| **Cybersecurity Providers** | Protecting customers; sharing threat intelligence; collaborating on disruption activities | Sharing technical threat intelligence, mitigations, and pushing those protections to customers; participating in incident response activities with customers |
| **Telecommunications/ISPs** | Protecting customers and maintaining networks | Identify malicious traffic, block malicious traffic, share threat intelligence |
| **Cloud Service Providers** | Protect the data stored on their networks; deny malicious actors a safe haven | Share threat intelligence data; take action on their own networks to disrupt malicious activity |
| **IT Companies** | Identify and patch vulnerabilities in their products | Issue patches for known vulnerabilities |
| **Critical Infrastructure Companies** | Protect key systems, technologies, and business processes and provide information related to their particular vantage point | Take actions on their own networks to ensure continuity of critical services |
| **Information sharing org. with cybersecurity capabilities and information** | Ensuring relevant information gets to the right recipients | Facilitating information flows, meetings; serve as a hub for communications and actions |
| **DOJ – FBI** | Threat response | Disrupt sophisticated malicious actors that pose a systemic risk |
| **DHS** | Coordination of U.S. government asset response and risk management support to critical infrastructure. | Work with private sector to design and operate programs to ensure whole of government capabilities brought to bear. Provide incident response. |
| **Office of the Director of National Intelligence and the Intelligence Community** | Intelligence and support | Collection support and analytic collaboration with operational collaboration partners to provide actionable intelligence including early warning. |
| **Department of Defense** | Contingency planning;<br>Offensive operations | Use DoD capabilities to disrupt threats from nation-state adversaries, when appropriate. |
| **Department of State** | Possible sanctions and other diplomatic efforts; negotiating norms of behavior for nation-state actors in cyberspace | Use diplomatic options to address/curtail disruptive or destructive threats from key nation-state adversaries |
| **Department of Commerce – NIST** | Standards, research | |
| **Department of the Treasury** | Economic sanctions | |
| **Executive Office of the President** | Public Policy | Coordinate and drive policy to support whole of government operational collaboration |
| **Congress** | Public Policy | If necessary, enable operational collaboration with legislative action |

### Table 2: Potential Actions to Support Mission Areas and Cross-cutting Enablers

| Function | Public | Private |
|---|---|---|
| **Intelligence and Information Sharing** | Focus technical intelligence, information sharing, and analytic collaboration with organizations and government agencies able to use it to protect themselves and others and to improve the quality of shared data and contribute to understanding threats | Identify use cases for threat intelligence sharing and define required data for each use case |
| **Risk Management** | Conduct research to model potential cross-sector systemic failures due to cyber incident | Collaborate in core research on potential cross-sector systemic failures |
| **Contingency Planning** | Create voluntary standards and best practices for public companies (e.g. NIST) | Develop model contingency plans for specific sectors |
| **Offensive Cyber Operations** | Establish a firm definition and ban on commissioning or engaging in offensive cyber operations by private entities. Develop contingency plans, in coordination with private sector when appropriate, that can be leveraged in exigent circumstances | Commit to not conducting; contribute to government-led efforts as appropriate. |
| **Policy (Public and Product)** | Create a legal framework for operational collaboration activities (anti-trust exemption; liability protection) | Adopt voluntary security standards for IOT products |