ACSC: Launched and supported by
Mass Insight

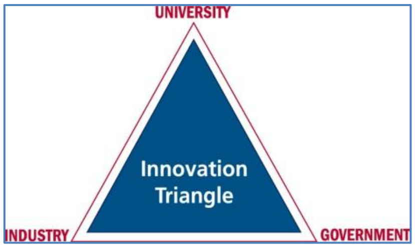
ADVANCED
CYBER SECURITY
CENTER
A National Center Hosted at The MITRE Corporation

Advanced Cyber Security Center Rollout

A proposal to address the Cyber Challenge by incentivizing and supporting industry initiatives rather than depending on legislation to improve our Cyber Defense posture

Who We Are

The Advanced Cyber Security Center (ACSC), a nonprofit corporation supported by Mass Insight Global Partnerships and based in Massachusetts, brings together industry, university, and government organizations to address the most sophisticated advanced cyber threats. Our focus is on developing and promoting greatly expanded cross-sector collaboration among New England institutions in order to develop an unprecedented critical mass to address the cyber threat. We are developing unique approaches to sharing cyber threat information, to engaging in next-generation cyber security research and development, and to creating education programs that will address the shortfall in cyber talent. All of these actions will help to protect the public and private information systems and critical infrastructure, both in New England and throughout the US.



The ACSC is currently 100% funded by our members, which include the six major Massachusetts research universities, the three regionally-based defense non-profits, and many of New England's most successful corporations.

The Need

The advanced cyber threat is real and growing. President Obama has said "… it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation." Any public or private sector organization is at risk of undetected attacks that can result in sensitive information being stolen. In addition, critical infrastructure that drives the nation's economy—from banking and transportation to water and power—is at risk from cyber-attacks. Current approaches to mitigate the threat are not sufficient. The need exists for improved awareness, staff development and training, and information sharing in the short-term and new forms of collaborative R&D and education in the longer-term. See attachment A for a summary of existing cyber threat sharing capabilities.

Our Vision

- Expand the ACSC model first developed in New England to help establish a scalable national model for cyber security threat sharing, research and development, education, and thought leadership.
- Build on the considerable cyber security strengths already existing in each region of the country by increasing the cross-industry collaboration necessary to address this broadly-based threat.
- Assure that each region's public and private sector organizations are early adopters of emerging technologies and practices to counter advanced cyber threats.
- Provide a cross-industry focal point for cyber security information sharing and collaboration while supporting R&D and educational programs that will lead to cyber security innovations, drawing top students and producing talented graduates in the process.

Foundations of our Strategy

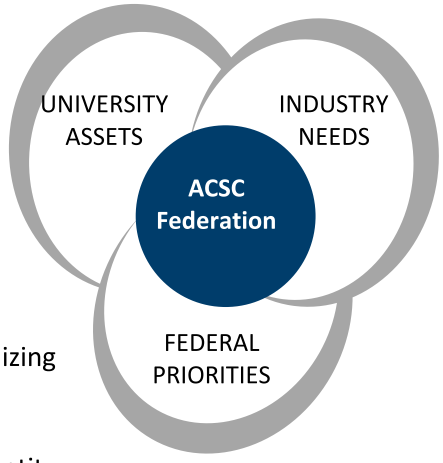
The ACSC Rollout strategy is built upon three key facts:

1. Cyber security is a national security and economic issue. Organizations of all sizes and in many different sectors are vulnerable to cyber attacks. These attacks are causing billions of dollars of damage to individuals and businesses, and cyber adversaries are stealing intellectual property and sensitive information that can impact economic and national security. The threat is based on a broad combination of technology, economic, legal, public policy, and national security issues. ***Addressing this threat will require a coordinated effort among many public and private organizations with diverse capabilities.***
2. ***A new national strategy that incentivizes and supports industry initiatives rather than depending on legislation best positions us to take on the cyber challenge***. Each region has a unique combination of leading public and private institutions with varying capabilities in high technology, management, law, economics, finance, human behavior, and public policy. All of these areas are critical for addressing the cyber threat.
3. The ACSC model employs a new research and information-sharing paradigm. The advanced cyber threat is too complex for any one entity to try to solve. ***The ACSC takes a collaborative approach in which a manageable group of organizations shares real-time information through trusted relationships and a non-disclosure agreement.*** Our universities connect with businesses on a pre-competitive basis, with the support and participation of government, to work together on next-generation research that shapes the commercial marketplace.

Specific Proposal

A national ACSC rollout could be accomplished with the following steps:

- Rollout four (4) regional ACSCs throughout the country to maintain the ACSC model, utilizing personal connections to create trusted relationships as the basis for cross industry sharing.
- Offer a matching program, providing $1 to 1 in federal funding to match private industry funding up to a maximum of $1M federal funding annually per regional entity to incentivize industry players to invest in their own cyber protection.
- Fund development of ACSC collaboration/support tools to create a federation of independent but cooperative ACSCs, utilizing similar threat repositories, legal agreements and management tools, minimizing redundant costs and maximizing speed of execution.
- Commit to three year program funding.
- Total three year federal cost of $12M. $1M/year for each regional entity.

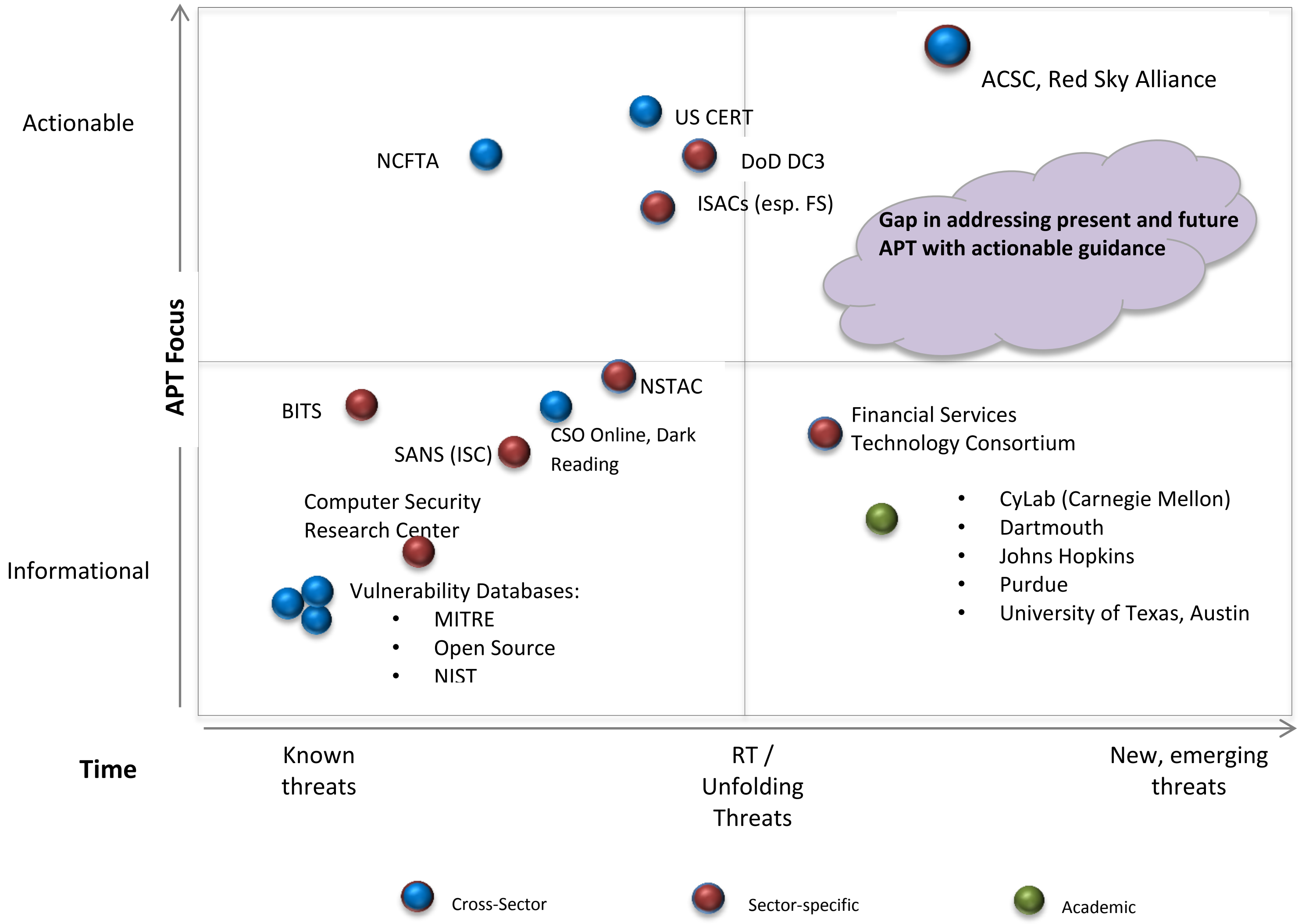


Next Steps

Representatives of Mass Insight and the ACSC will be happy to meet to discuss next steps.

Attachment A

Existing Collaborations



Source: ACSC Directed External Research