Office of Cybersecurity and Communications (CS&C)

Dr. Peter Fonash
Chief Technology Officer (CTO)

Strengthening the Cyber Ecosystem

Presented to IEEE Computer Society Rock Stars of Cybersecurity
24 September 2014

What is the *Cyber Ecosystem*?

The cyber ecosystem is global, evolving and includes government and private sector information infrastructure; the interacting people, processes, data, information and communications technologies; and the environment and conditions that influence their cybersecurity

Physical and Cyber Resiliency Components of the Cyber Ecosystem

- Physical (well understood & risk managed)
  - Supporting infrastructure (i.e., power, water, etc) 🟩
  - Communications 🟩
  - Hardware 🟩
  - Software 🟩
  - Human organizational 🟩
- Cybersecurity (evolving)
  - Supporting infrastructure (i.e., power, water, etc) 🟨
  - Communications 🟩
  - Hardware 🟩🟨
  - Software 🟨
  - Human organizational 🟨🟥
  - Data confidentiality integrity and availability 🟨

Strengthening the Cyber and Communications Ecosystem for the Future

Today

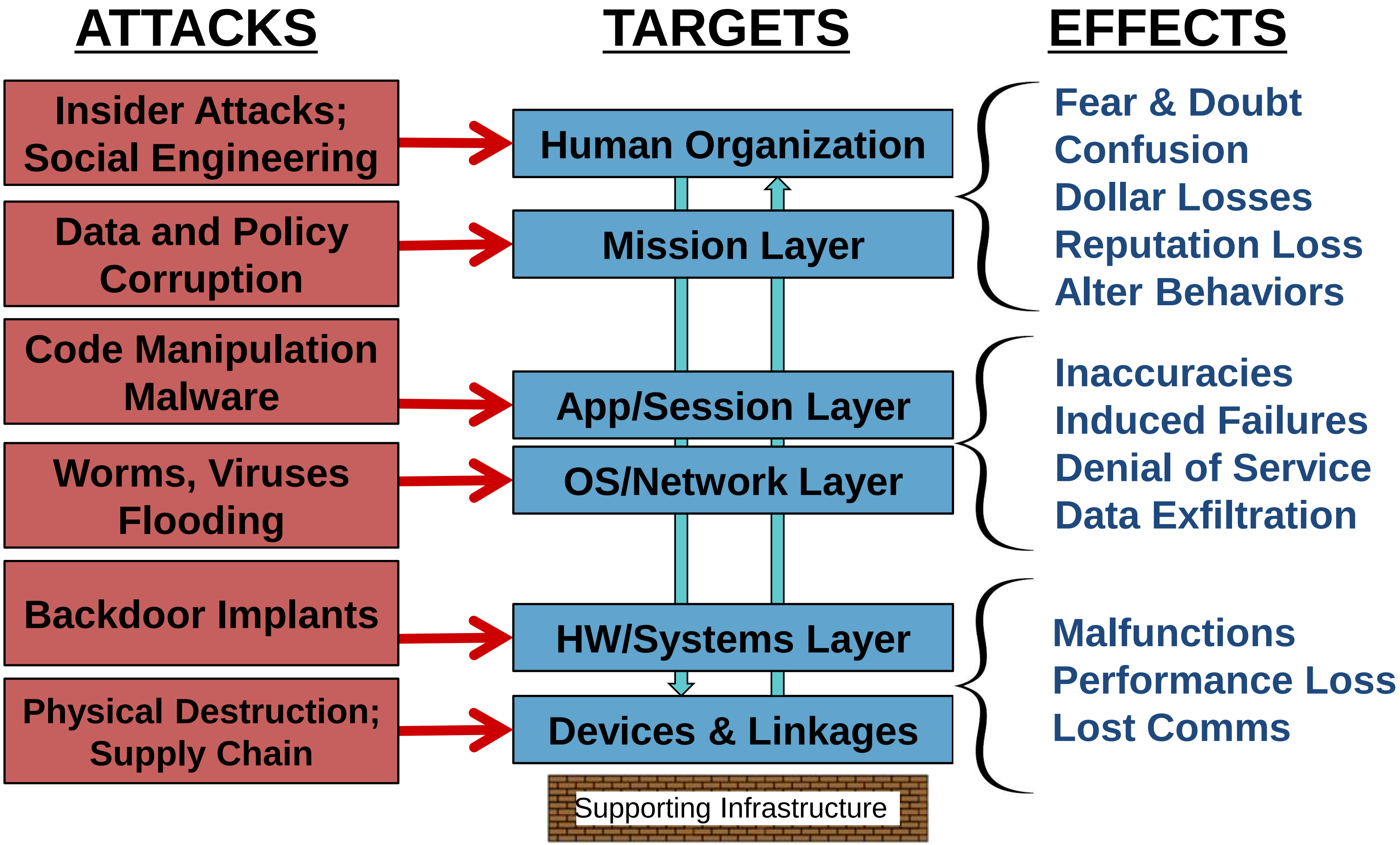
- Many unknown vulnerabilities
- Incidents spread at network speed and defenses are manual
- Many attacks are undetected
- Independently defended systems
- Inconsistent security policies
- Users do not follow best practices
- Attacks increasing in number and virulence
- Non-interoperable proprietary solutions
- Defenses not integrated or interoperable

Future

- Baked in security = fewer vulnerabilities
- Near real-time response with more automated defenses
- Many attacks, but less impact
- Information sharing and increasingly collaborative defenses
- Consistent security practices
- Unauthorized activity quickly identified
- Ability to learn and adapt defenses in near-real time
- Plug and play interoperable architecture fostering innovation

Adversaries will continue to have robust and evolving capabilities

The Challenge: Cyber Attacks, Targets, Effects



ATTACKS

Insider Attacks; Social Engineering

Data and Policy Corruption

Code Manipulation Malware

Worms, Viruses Flooding

Backdoor Implants

Physical Destruction; Supply Chain

TARGETS

Human Organization

Mission Layer

App/Session Layer

OS/Network Layer

HW/Systems Layer

Devices & Linkages

Supporting Infrastructure

EFFECTS

Fear & Doubt
Confusion
Dollar Losses
Reputation Loss
Alter Behaviors

Inaccuracies
Induced Failures
Denial of Service
Data Exfiltration

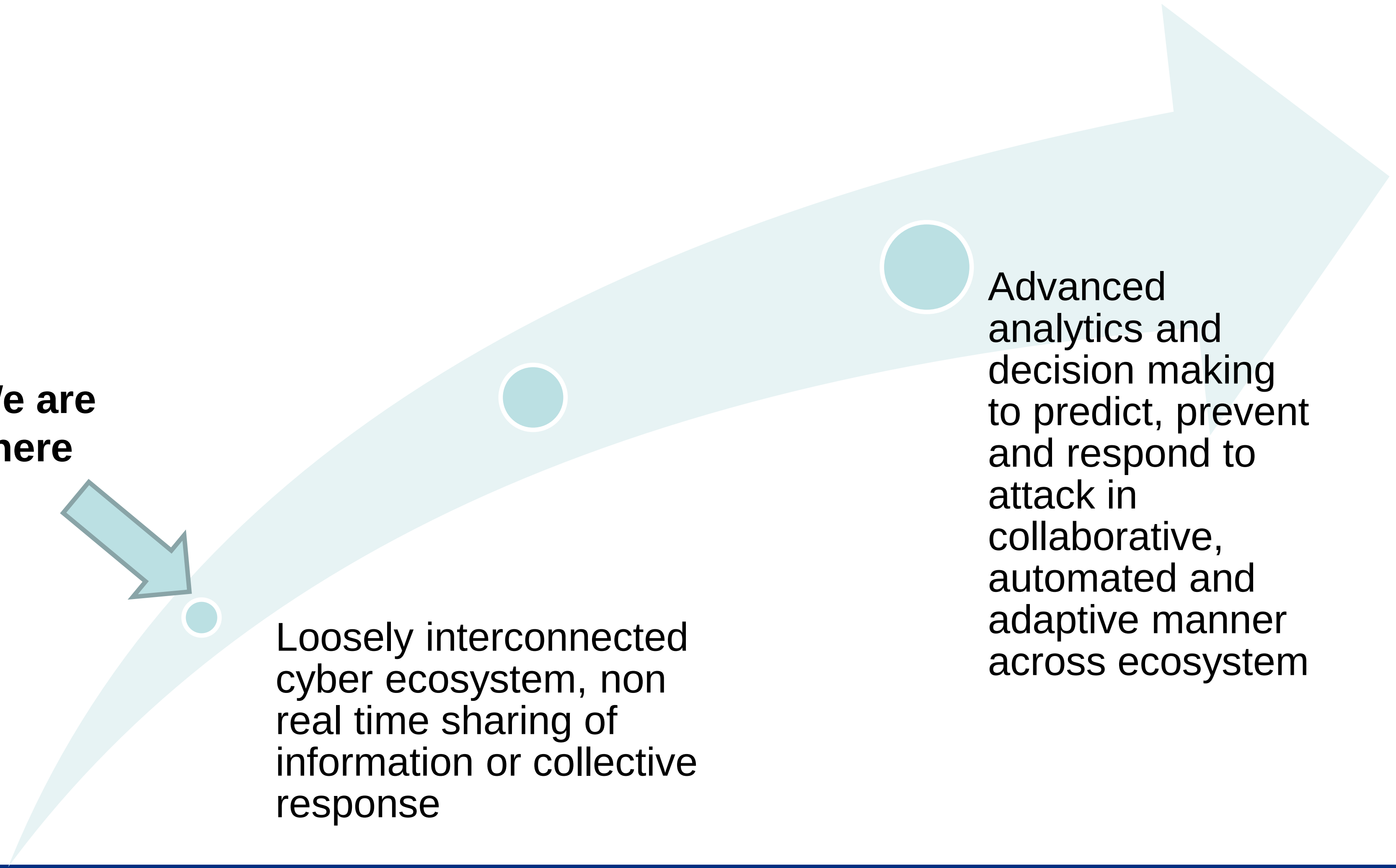
Malfunctions
Performance Loss
Lost Comms

Modified From AF SAB Cyber Report, 2008

Strengthening the Cyber Ecosystem

- Weather Map
  - Situation awareness--information sharing
  - Improved analytics based on “big data analytics”
  - Collective action based on shared information
- Automated & Adaptive Capabilities
- Greater Effectiveness & Integration
  - Integrated tools
  - Response from months to seconds
  - Plug & play technology/interoperability
  - Signature/Reputation/Behavior based detection

Where are we: Ecosystem Evolution



We are here

Loosely interconnected cyber ecosystem, non real time sharing of information or collective response

Advanced analytics and decision making to predict, prevent and respond to attack in collaborative, automated and adaptive manner across ecosystem

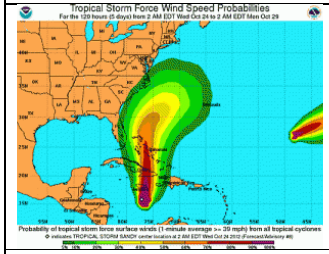
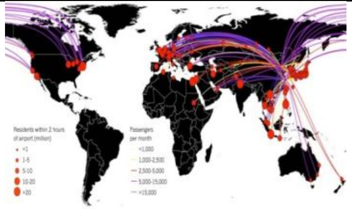
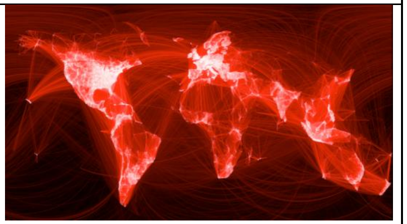
Why is a Cyber Weather Map Needed?

- Supports Identify, Protect, Prevent, Detect and Respond/Recover
  - Situation awareness and common operational picture
- Aggregation of data enables “Big Data Analytics”
- Weather Map informs and facilitates collective automated response
- Parallels exist in other areas (disease control)

Why should DHS do a Weather Map?

- Most diverse and unique sources of cyber data
- DHS has established partnerships and information sharing role
- Facilitates our Identify, Protect, Prevent, Detect, Respond and Recover roles
- Infrastructure established and funded (in out years)

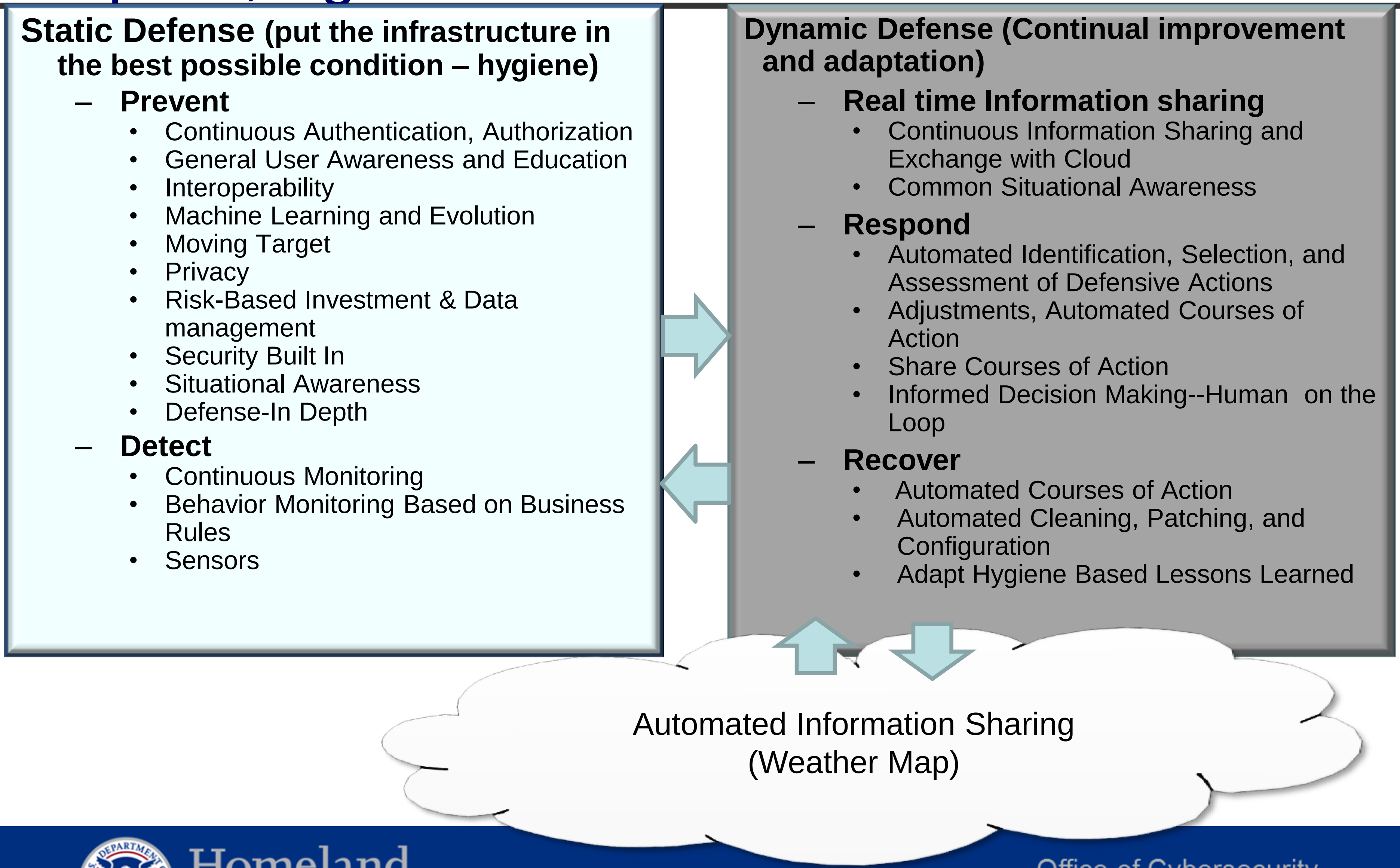
Precedent for a DHS Weather Map

NOAA	CDC	FAA	DHS
			
• Collection of weather related data • Storage of many years of data • Collect most recent weather data from all available relevant sources • Analysis of interrelated data points with possible impacts on weather changes • Statistical modeling to create prediction of future changes to current weather based upon past history • Provide both raw data and weather predictions to large variety of users • Provide mitigation recommendations to areas with potential impacts	• Collect medical data related to contagious diseases • Store all collected data • Analyze possible relationships of medical information • Collect most recent medical information with potential contagious possibilities from as many sources as possible • Track efforts to control spread of disease • Continuously analyze changes in information being collected • Utilize modeling to create prediction of future spread of disease. • Provide recommendations to mitigate future spread of disease	• Collect information related to all aircraft, airfield, and traffic related incidents • Store all collected data • Select all data related to an accident and incident • Analyze current and past related information to determine possible causes • Recommend changes to mitigate future incidents and accidents	• Collect all relevant cyber information ○ .gov ○ Anonymized from Sectors, Industry, States, etc. • Store in appropriate data bases relevant to user access controls • Collect non-cyber information that may be relevant in predicting potential future attacks • Analyze data for patterns and anomalies for determining potential threats • Provide/collect raw and analyzed information to/from relevant stakeholders • Provide, describe, or obtain mitigation measures to/from stakeholders • Recommend legal/policy changes to improve cyber security
Reduces physical damage. Saves lives. Allows for preparation time.	Reduces sickness & death. Saves expenses.	Reduces airline incidents. Reduces physical damage. Saves lives.	Provides warning of potential attack Reduces financial losses, equipment damage, information losses, and secondary impacts such as power loss, water contamination, etc.

Weather Map Challenges

- CS&C has some limited ability to forecast near-future ongoing cyber-threats, but little ability to predict out-year threats and trends
  - Nascent science
- Different sources of data have different use requirements
- For improved forecasting prediction capabilities, need:
  - More data… increase in data points, by being more trusted as a data broker with a global reach
  - More diverse data, accepted and used (today data of many types is discarded if collected at all)
  - Improved understanding of significance (diagnostic value) of data
  - Improved modeling and computation capabilities
  - Have to accept that data precursor-to-effect relationships are far less consistent than in other domains, so unknown threats will always be major factors
  - To defend in depth, need improved defenses that would function against even unknown threats

Objective State: Informed Risk Management & Adaptive, Agile Defense



Static Defense (put the infrastructure in the best possible condition – hygiene)

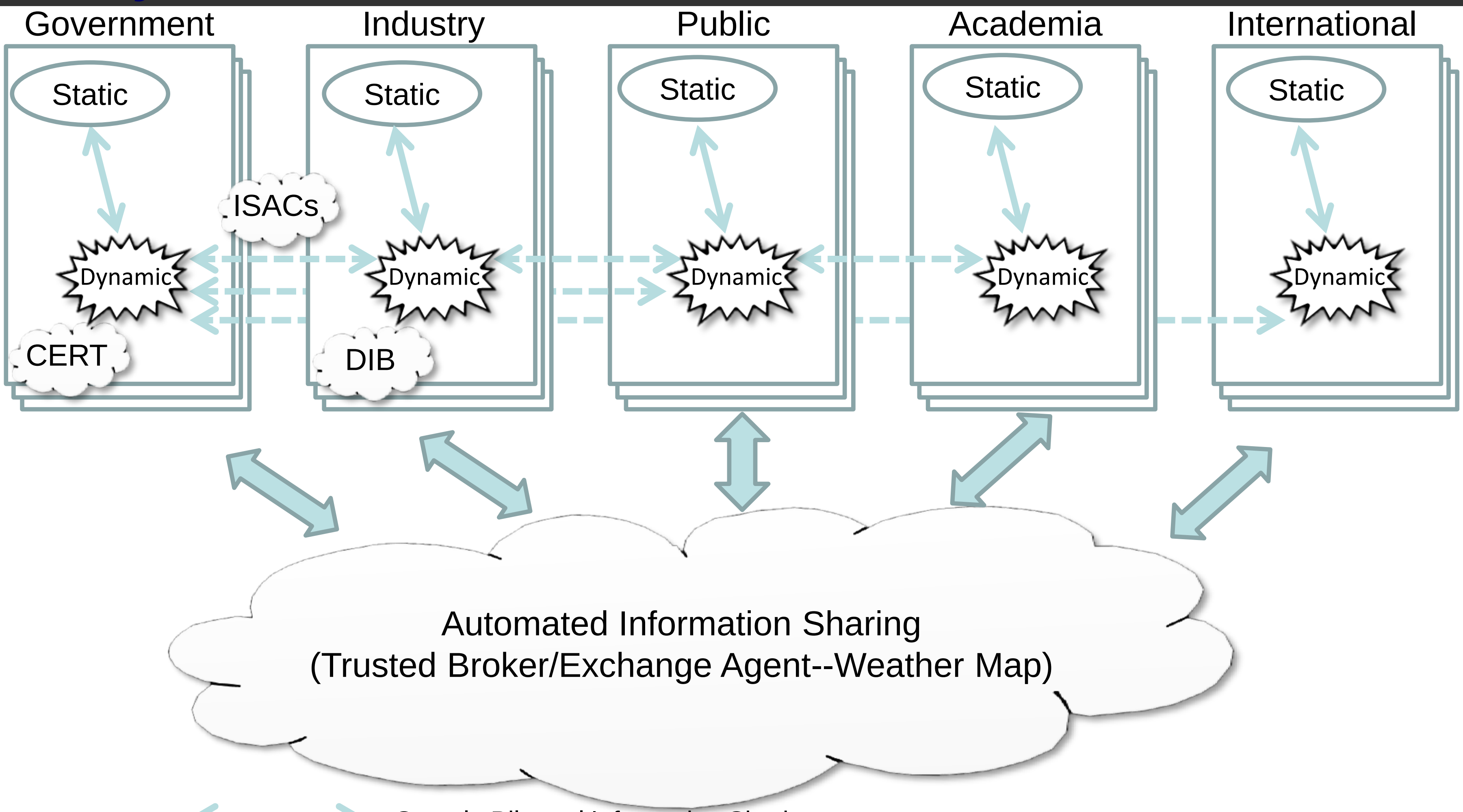
- **Prevent**
  - Continuous Authentication, Authorization
  - General User Awareness and Education
  - Interoperability
  - Machine Learning and Evolution
  - Moving Target
  - Privacy
  - Risk-Based Investment & Data management
  - Security Built In
  - Situational Awareness
  - Defense-In Depth
- **Detect**
  - Continuous Monitoring
  - Behavior Monitoring Based on Business Rules
  - Sensors

Dynamic Defense (Continual improvement and adaptation)

- **Real time Information sharing**
  - Continuous Information Sharing and Exchange with Cloud
  - Common Situational Awareness
- **Respond**
  - Automated Identification, Selection, and Assessment of Defensive Actions
  - Adjustments, Automated Courses of Action
  - Share Courses of Action
  - Informed Decision Making--Human on the Loop
- **Recover**
  - Automated Courses of Action
  - Automated Cleaning, Patching, and Configuration
  - Adapt Hygiene Based Lessons Learned

Automated Information Sharing
(Weather Map)

Automated Collective Action throughout the Ecosystem



<- - - - -> Sample Bilateral Information Sharing
Static = Static Defense (best hygiene)
Dynamic = Dynamic Defense (based on situational awareness)

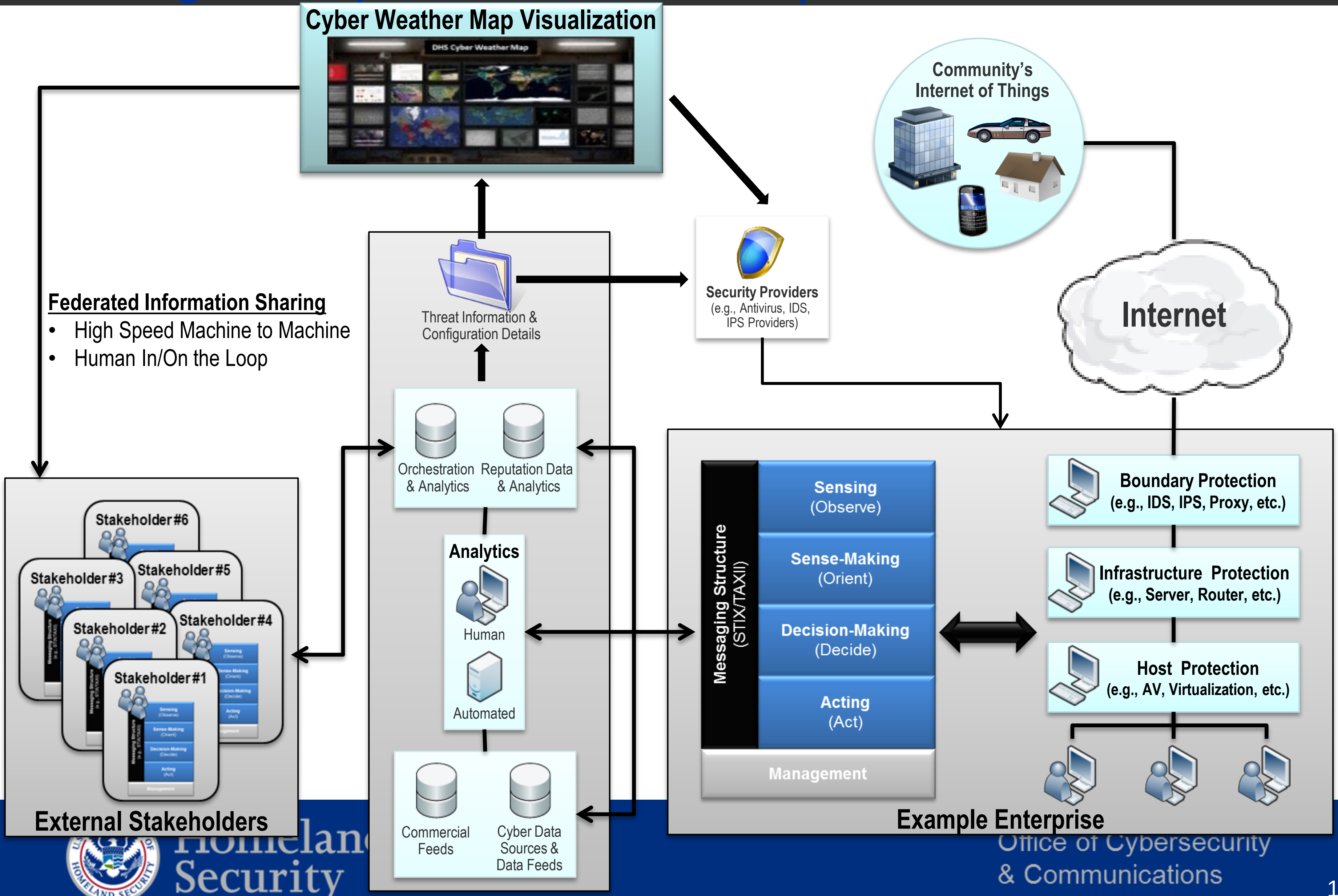
Key Comparisons---Cyber Challenges

	NOAA-NWS	NIH/CDC	DHS/CS&C
Data Context	• Weather is generally cyclical and broadly predictable. Specific events (Tornado path) may be difficult to predict in specific detail more than minutes or hours beforehand • Historic data is highly relevant to future probabilities	• Epidemics are somewhat cyclical and predictable. Specific details may be highly unpredictable but once identified, the epidemiology may be predictable. • Data is sometimes useful for forecasting disease category evolution and highly relevant to understanding epidemiology and public health consequences.	• Some data is a poor predictor of future activity. • The near-future course of an ongoing identified attack can often be forecast. Some successful forms of cybercrime and attacks persist for years, and may be predictable in the aggregate, but difficult to predict specifically. • Unique major threats may be intentionally unpredictable.
Structural Context	• Human activity may have large scale (e.g. changes in regional environment due to agriculture; Global warming) and small scale changes (local effects due to urban build-up) • Outlier climate events volcanoes, nuclear war, large-meteors.	• The disease agent and vector may each evolve in response to human activity, rendering current defenses ineffective. • Outlier events include evolution of new virulent organisms, or biological attack as acts of war.	• Specific attacks may be adapted or otherwise be changed quickly in response to defensive intervention. • Attack methods and practices may evolve over time in response to intervention. • Attacks of new types must be assumed to be in constant development. • Outlier: Coordinated attacks by cyber-weapons as acts of war.

Key Comparisons ---Cyber Challenges, Continued

	NOAA-NWS	NIH/CDC	DHS/CS&C
Data collection and integration	• Decades of highly relevant historical data available. • Trusted data broker.	• Decades of relevant historical data available • Data meaning may be sometimes obfuscated by similar symptoms, epitophy, etc. • Trusted data broker.	• Very little historical data • Early stages of defining what data is relevant and how to use • Significant progress and momentum on data standards and metrics • Issues of access, data protection, disclosure, legal and regulatory frameworks need to be addressed
Multi-scale modeling and forecasting	• Physics-based • Models have been validated and improved over time	• Epidemiology Models have been validated and improved over time. • Public health models have been validated and improved over time • Use of wide range of data (e.g. weather data to predict Malaria vector-mosquito population, National Retail Data Monitor to track OTC medicine sales)	• Assessments based on trade-craft and expert heuristics versus rigorous models • Analytical frameworks very immature • Analysis requires understanding of complex relationships between technology and people (security personnel, adversaries)

Goal: Integrated Adaptive Cyber Defense (IACD): Enabling Enterprise Owners & Operators



Cyber Weather Map Visualization

Community's Internet of Things

Federated Information Sharing

- High Speed Machine to Machine
- Human In/On the Loop

Threat Information & Configuration Details

Security Providers (e.g., Antivirus, IDS, IPS Providers)

Internet

Orchestration & Analytics

Reputation Data & Analytics

Analytics

Human

Automated

Commercial Feeds

Cyber Data Sources & Data Feeds

Stakeholder #6

Stakeholder #3

Stakeholder #5

Stakeholder #2

Stakeholder #4

Stakeholder #1

External Stakeholders

Messaging Structure (STIX/TAXII)

Sensing (Observe)

Sense-Making (Orient)

Decision-Making (Decide)

Acting (Act)

Management

Boundary Protection (e.g., IDS, IPS, Proxy, etc.)

Infrastructure Protection (e.g., Server, Router, etc.)

Host Protection (e.g., AV, Virtualization, etc.)

Example Enterprise

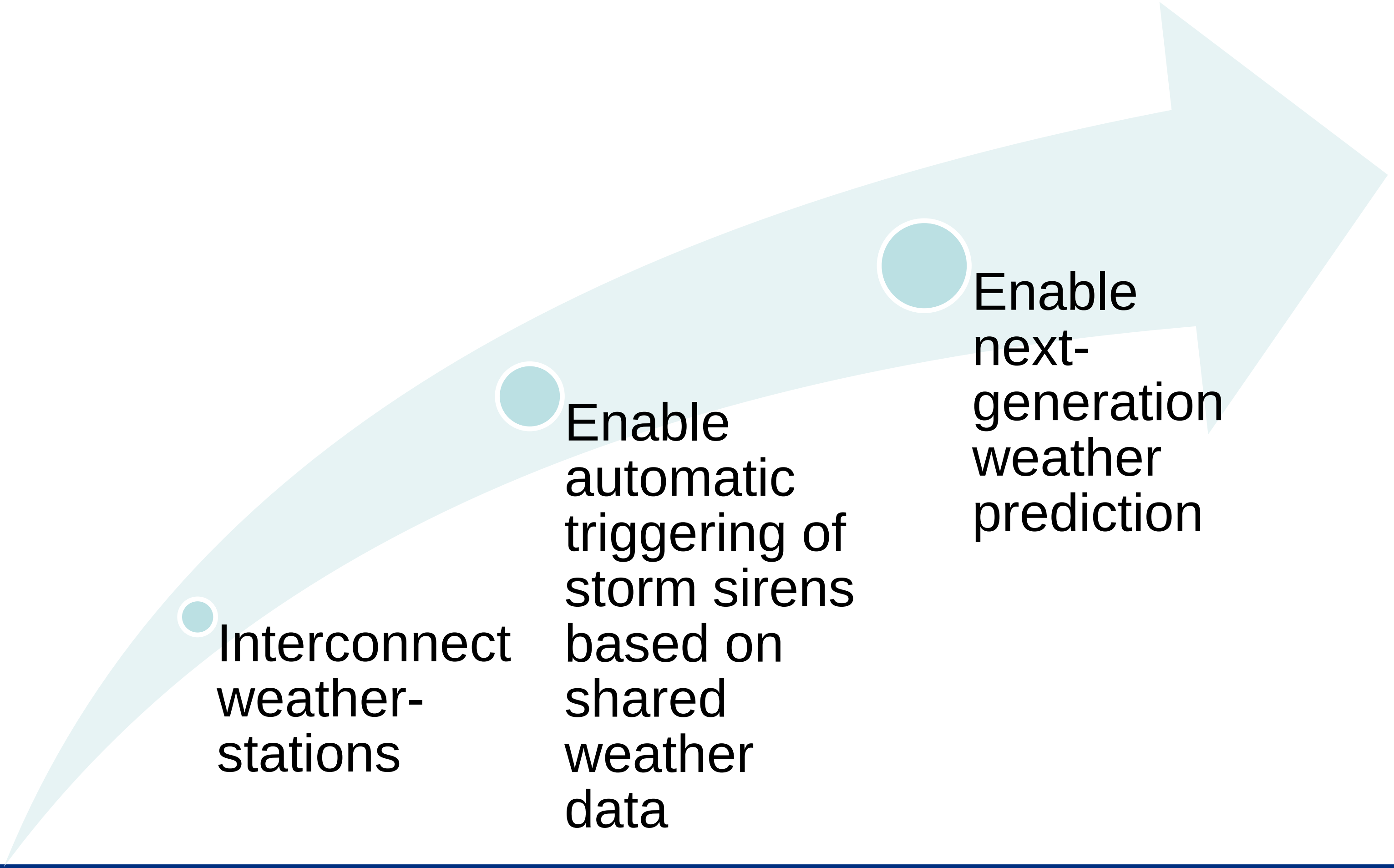
Summary

Success requires:

- Common situation awareness based on real time information sharing
- Collaborative automated courses of action based on common awareness and trust
- Effective and efficient tools
  - Integrated tools & data framework
  - Common data model
  - Low barriers to innovation
  - Adaptive sensing, sense making, decision making & courses of action

Backup Slides

In Meteorological Terms



Interconnect weather-stations

Enable automatic triggering of storm sirens based on shared weather data

Enable next-generation weather prediction

Define the Layers

Human and Organization: The mission is executed at this layer

Mission: Includes mission capabilities such as command and control or weapon systems

Application and Session: Includes applications such as databases and web browsers

Operating System and Network: Protocols and components such as routers and firewalls, along with their associated operating software

Hardware and Systems: Central processing units (CPUs) and storage arrays

Devices and Linkages: Materials and devices that provide the underpinnings of computing devices and networks. This layer includes communication links and electronic devices such as wires, antennas, transistors, and chips