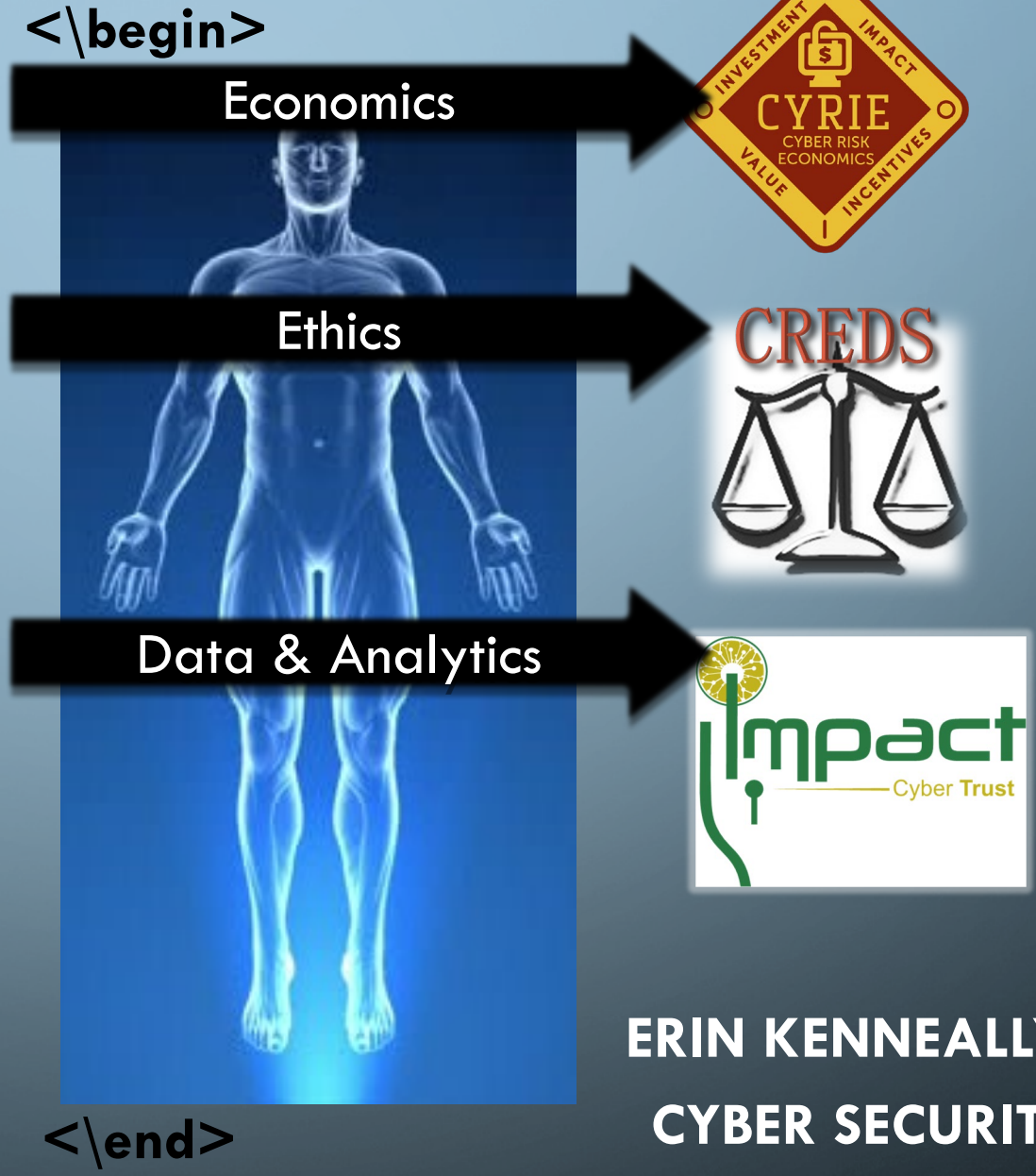
CYBER RISK R&D ENABLING TRUSTED CYBERSECURITY INNOVATION



Homeland Security

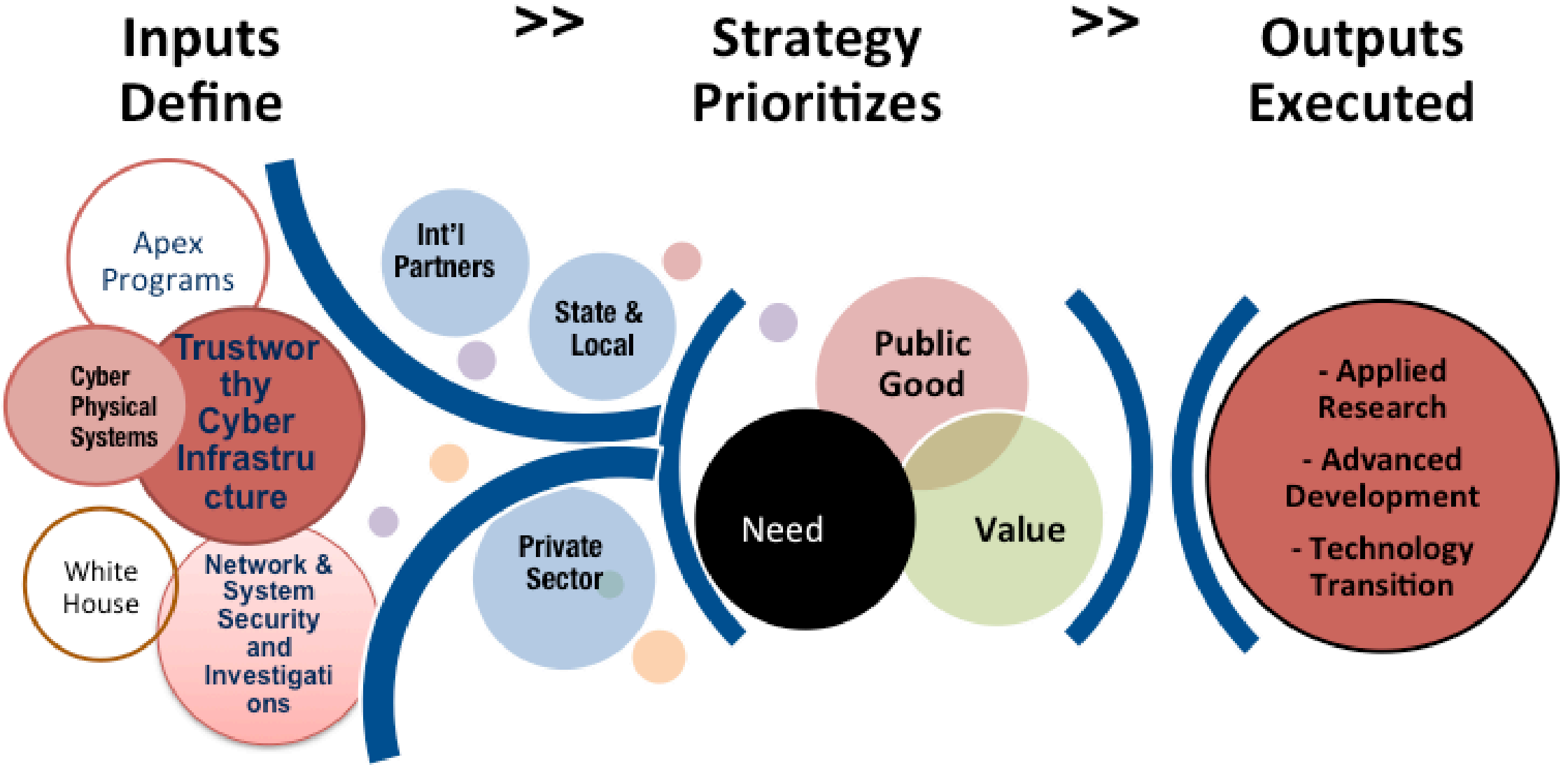
Science and Technology

ERIN KENNEALLY, M.F.S., J.D.

CYBER SECURITY DIVISION

Homeland Security

Science and Technology



The Penalty Stroke Effect

Information Marketplace for Policy and Analysis of Cyber-risk & Trust

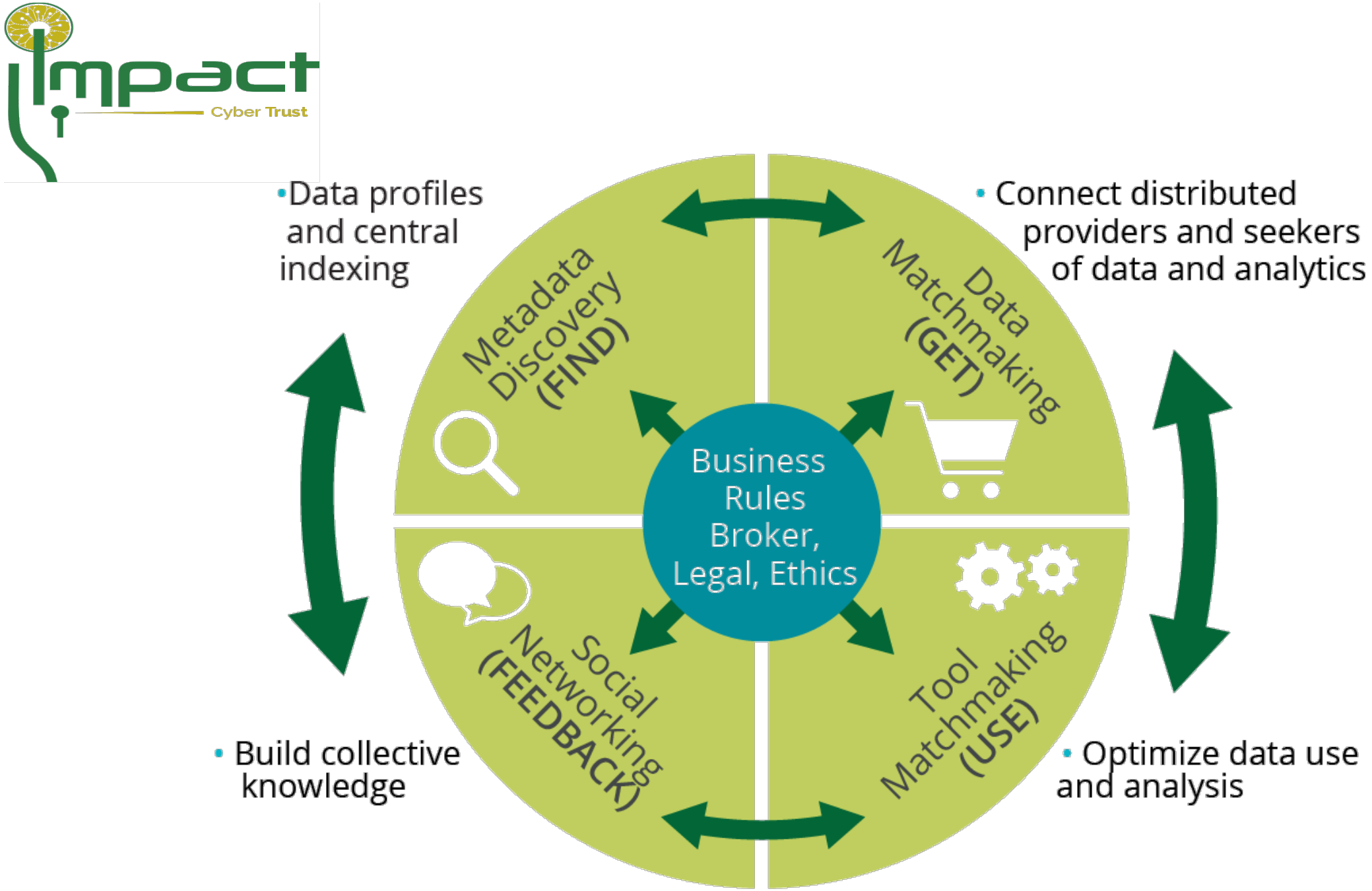
Capability Need: Open Secret of Effective R&D

- **Data are critical to R&D capabilities**
  - Cybersecurity needs real-world data to develop, test, evaluate knowledge & tech solutions to counter cyber threats
  - "Big Data" may grow on trees … still has to be picked, sorted, trucked
  - Most researchers are on "Datacaid"

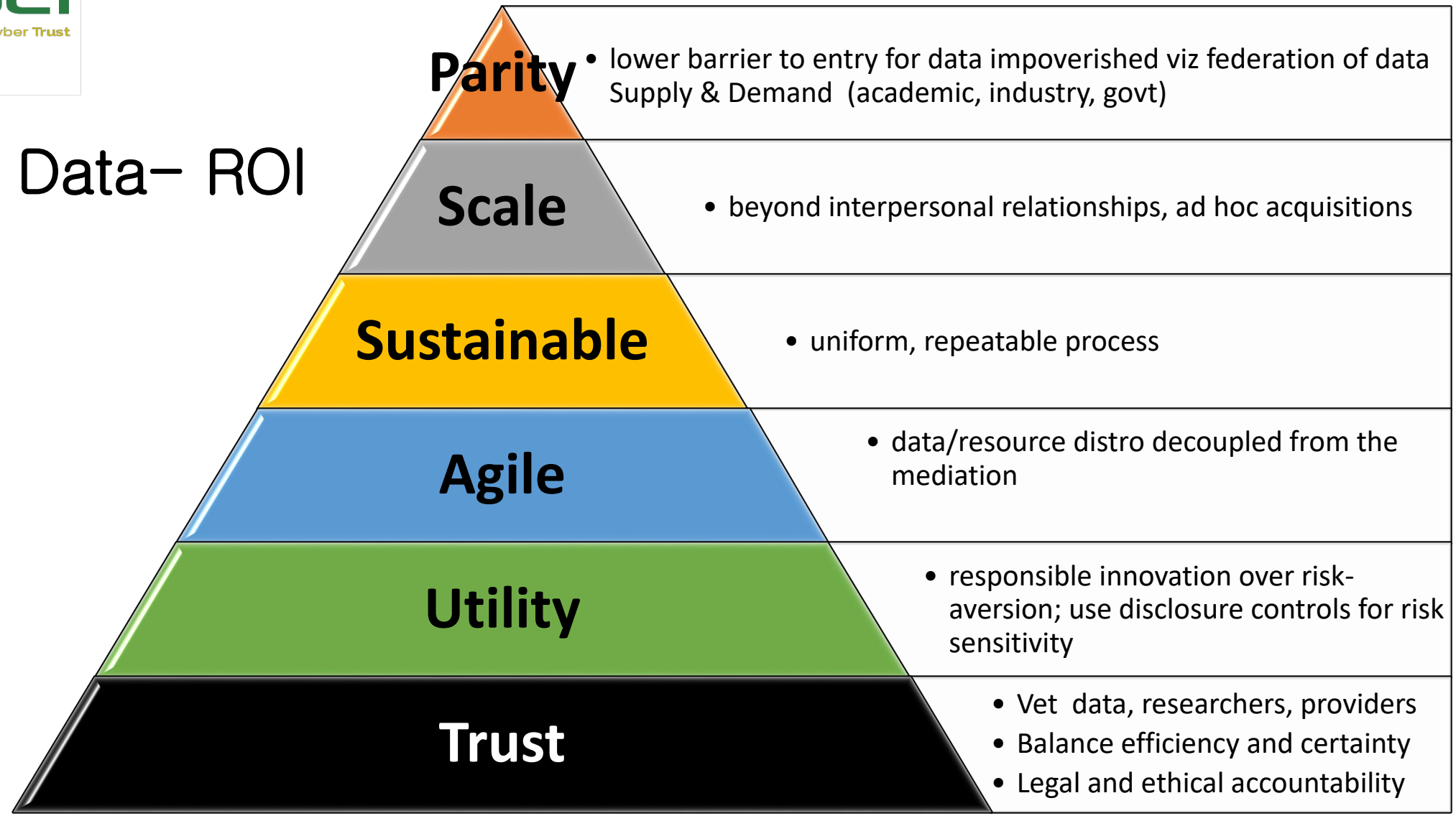
- **Decision analytics are critical to Govt and Industry capabilities**
  - Cybersecurity needs integrated, holistic understanding of risk environment
  - Gap between Data <-->Decisions: multi-dimensional, complex association and fusion, high-context presentation elements

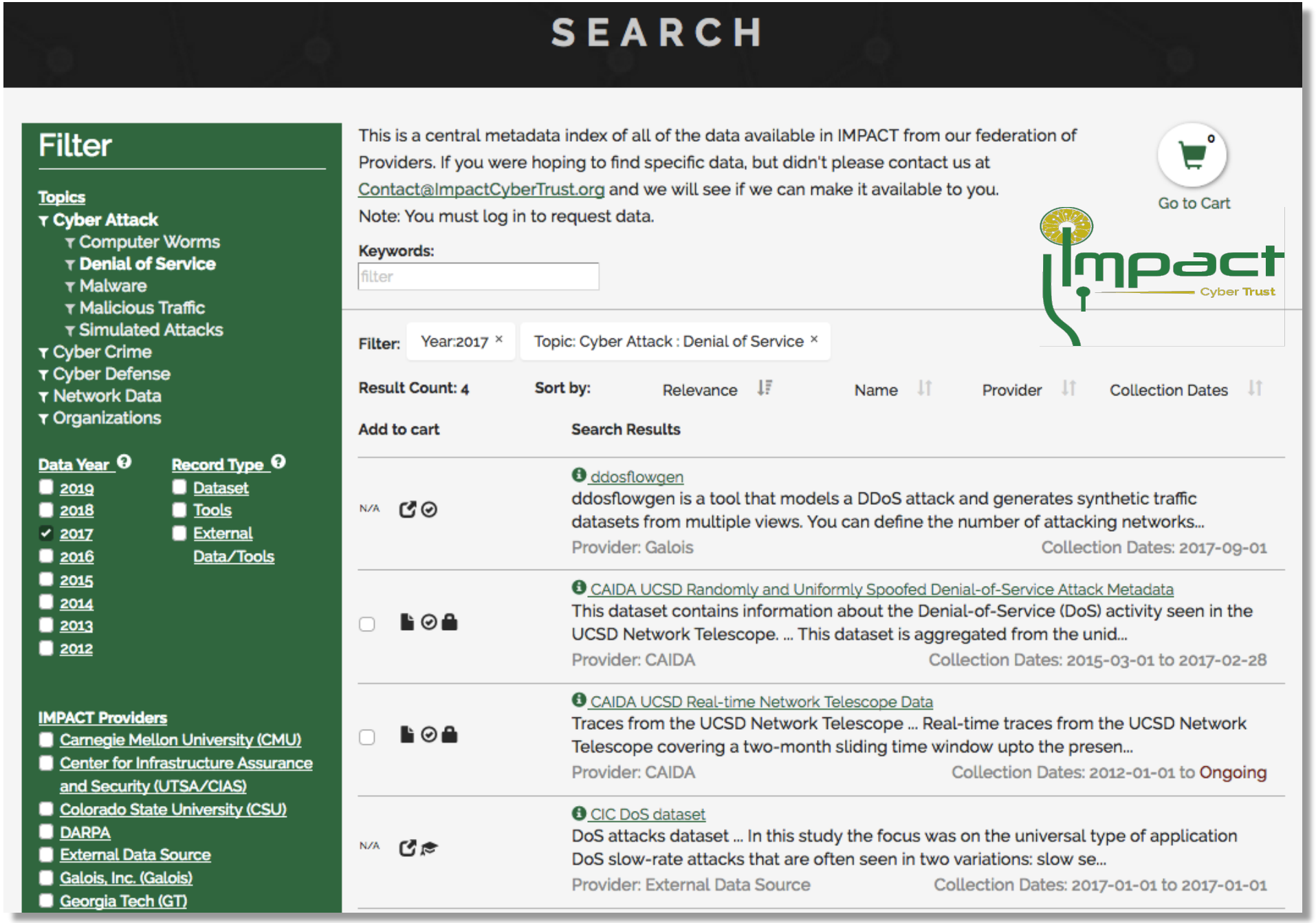
- **But, Data sharing +**

  Decision Support|= Easy
  - High value data = High legal risk + $$
  - Expensive to abstract away low level knowledge- and labor-intensive tasks
  - Techies optimize for Efficiency, Lawyers optimize for Certainty


Data profiles and central indexing
Connect distributed providers and seekers of data and analytics
Metadata Discovery (FIND)
Data Matchmaking (GET)
Business Rules Broker, Legal, Ethics
Social Networking (FEEDBACK)
Tool Matchmaking (USE)
Build collective knowledge
Optimize data use and analysis

Enabling Data– ROI

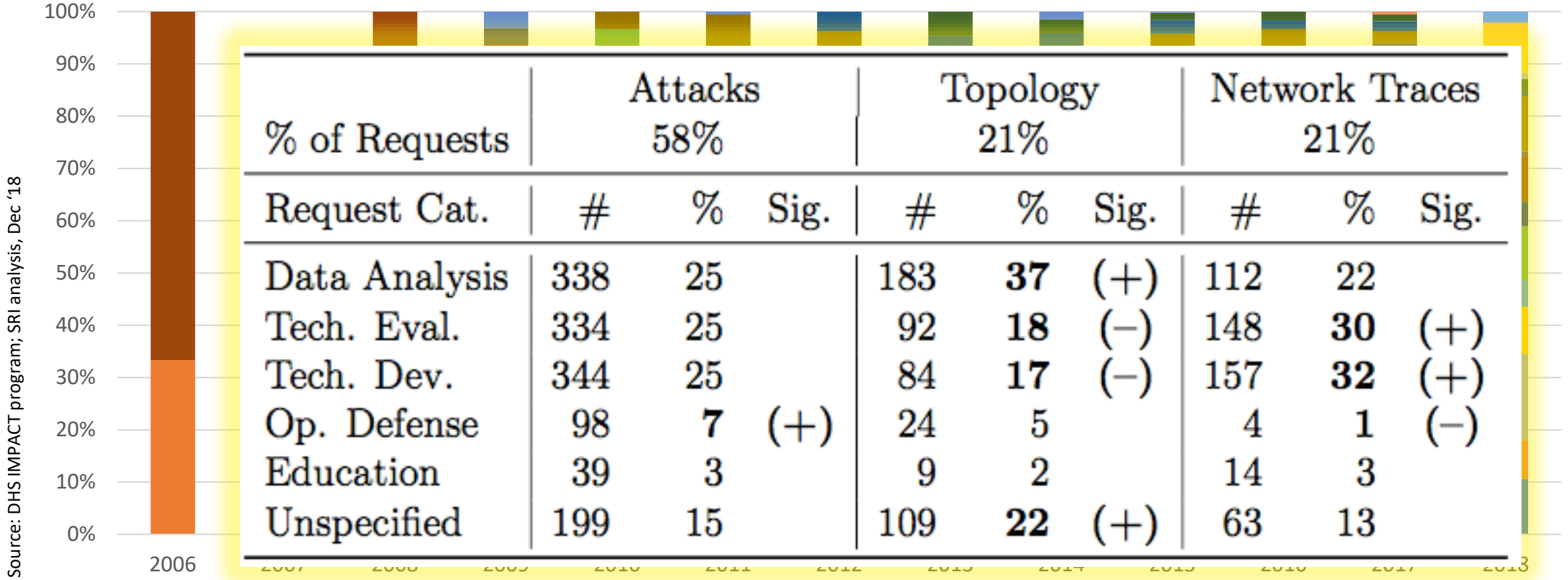




Shop ‘til You Drop
IMPACT Portal

ImpactCyberTrust.org

Data Trends



% of Requests	Attacks 58%			Topology 21%			Network Traces 21%		
Request Cat.	#	%	Sig.	#	%	Sig.	#	%	Sig.
Data Analysis	338	25		183	**37**	(+)	112	22	
Tech. Eval.	334	25		92	**18**	(−)	148	**30**	(+)
Tech. Dev.	344	25		84	**17**	(−)	157	**32**	(+)
Op. Defense	98	**7**	(+)	24	5		4	**1**	(−)
Education	39	3		9	2		14	3	
Unspecified	199	15		109	**22**	(+)	63	13	

Source: DHS IMPACT program; SRI analysis, Dec '18

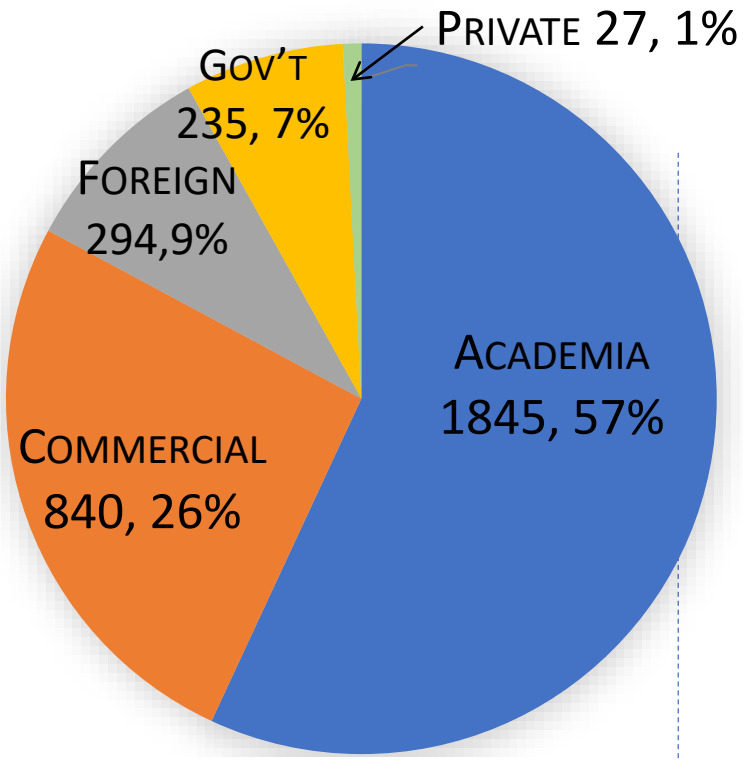
- DNS DATA
- TRAFFIC FLOW DATA
- SYNTHETICALLY GENERATED DATA
- ADDRESS SPACE STATUS DATA
- INFRASTRUCTURE DATA
- IP PACKET HEADERS
- UNSOLICITED BULK EMAIL DATA
- BLACKHOLE ADDRESS SPACE DATA
- BGP ROUTING DATA
- INTERNET TOPOLOGY DATA
- CYBERSECURITY CONTROLS DATA
- GEOLOCATION DATA
- PERFORMANCE AND QUALITY MEASUREMENTS
- APPLICATION LAYER SECURITY DATA
- ATTACKS
- CYBERCRIME INFRASTRUCTURE
- OTHER

Data Popularity (2015-18)

Dataset Name	Data Provider
GT Malware Passive DNS Data Daily Feed	Georgia Tech
US Long-haul Infrastructure Topology	University of Wisconsin
GT Malware Unsolicited Email Daily Feed	Georgia Tech
DARPA Scalable Network Monitoring (SNM) Program Traffic	DARPA
Historical GT Malware Passive DNS Data 2011-2013	Georgia Tech
CAIDA DDoS 2007 Attack Dataset	UCSD - Center for Applied Internet Data Analysis
Skaion 2006 IARPA Dataset	University of Southern California-Information Sciences Institute
DSHIELD Logs	University of Wisconsin
CAIDA UCSD Real-time Network Telescope Data	UCSD - Center for Applied Internet Data Analysis
syn-flood-attack	Merit Network, Inc.
DoS_traces-20020629	University of Southern California-Information Sciences Institute
DoS_80_timeseries-20020629	University of Southern California-Information Sciences Institute
Netflow-1	Merit Network, Inc.
NCCDC 2013	Center for Infrastructure Assurance and Security (UTSA/CIAS)
NCCDC 2014	Center for Infrastructure Assurance and Security (UTSA/CIAS)
Insider Threat Data Corpus 2016	University of Southern California-Information Sciences Institute
Netflow-2	Merit Network, Inc.
Netflow-3	Merit Network, Inc.
NCCDC 2015	Center for Infrastructure Assurance and Security (UTSA/CIAS)

Global, Multi-Sector "Impact" (as of February 2019)

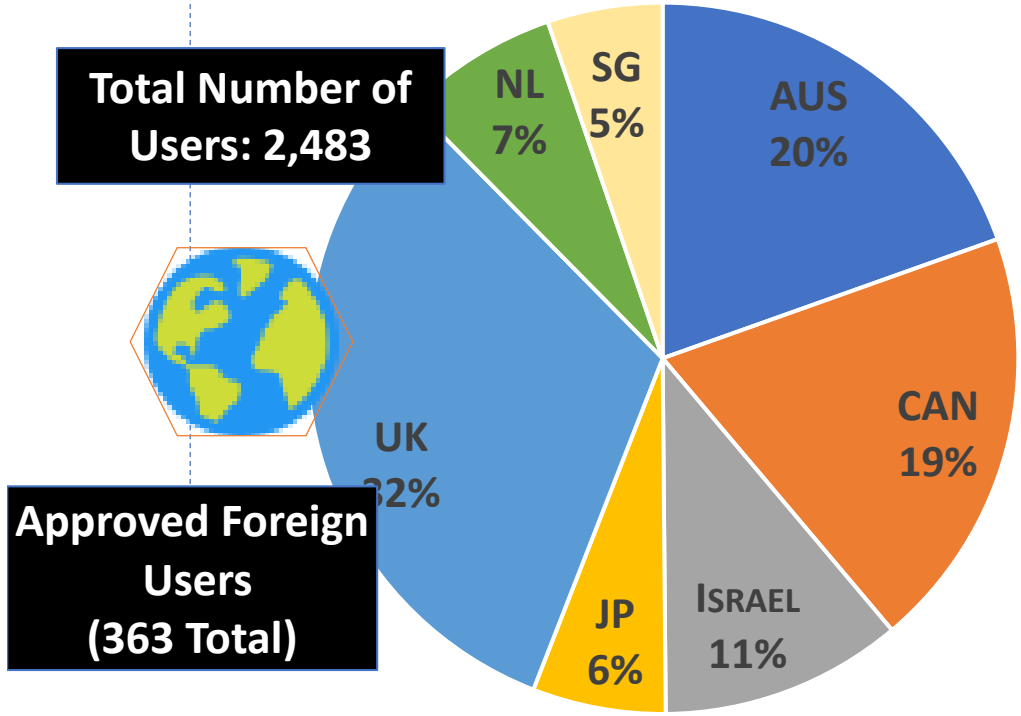
Dataset Requests By User Type (Total: 3,241)



Dataset Provisioned (>3,800)

Research papers, journals, tech reports (>300 "known")

Total Number of Users: 2,483



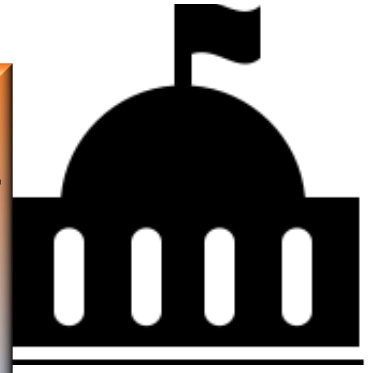
Approved Foreign Users (363 Total)

Source: DHS IMPACT program; SRI analysis, 2018-19

Example Success Stories

* OCIA: Internet Capability Project (Internet Topology)

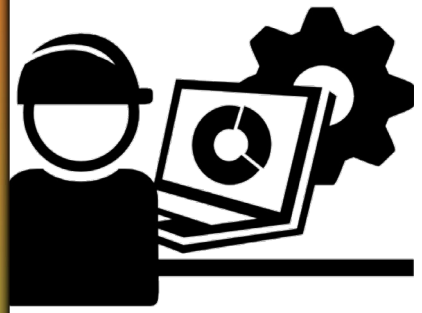
* CISA: Internal Ops (Internet Atlas, MPDNS)



* Galois: 3DCoP ISP DDoS defense

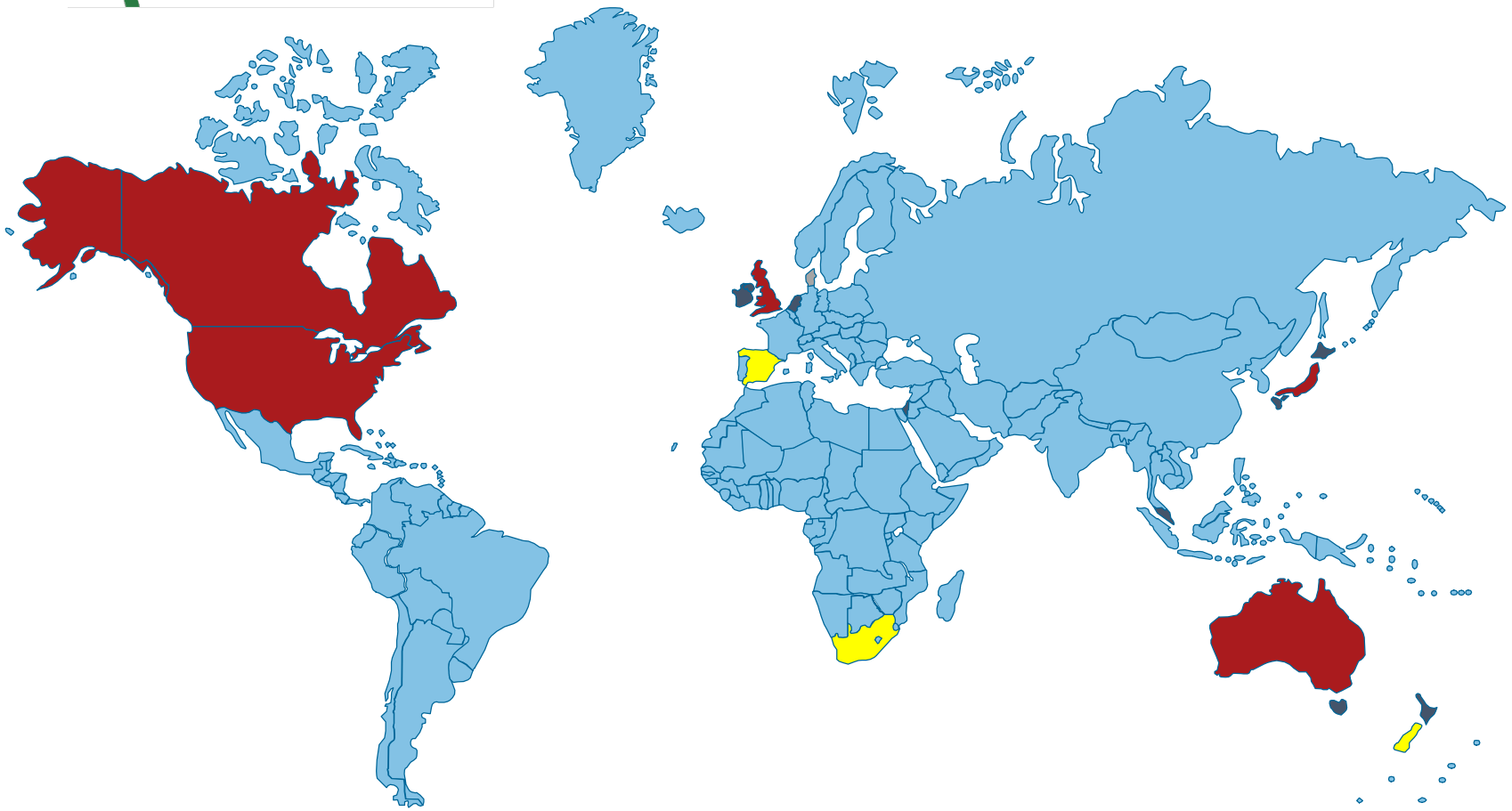
* Comcast: understand scanning for vulnerable IoT devices

* Most major AV vendors consume daily malware feeds



* Ph.D. Thesis, Conference paper, Zhan
A characterization of cybersecurity posture from Network Telescope data

Customers & Stakeholders

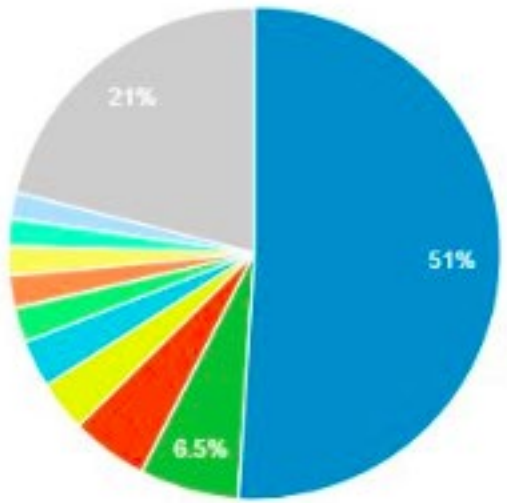


IMPACT customer base encompasses cyber security researchers and developers in 8 partner countries: AUS, CAN, UK, JA, NL, Israel, Singapore

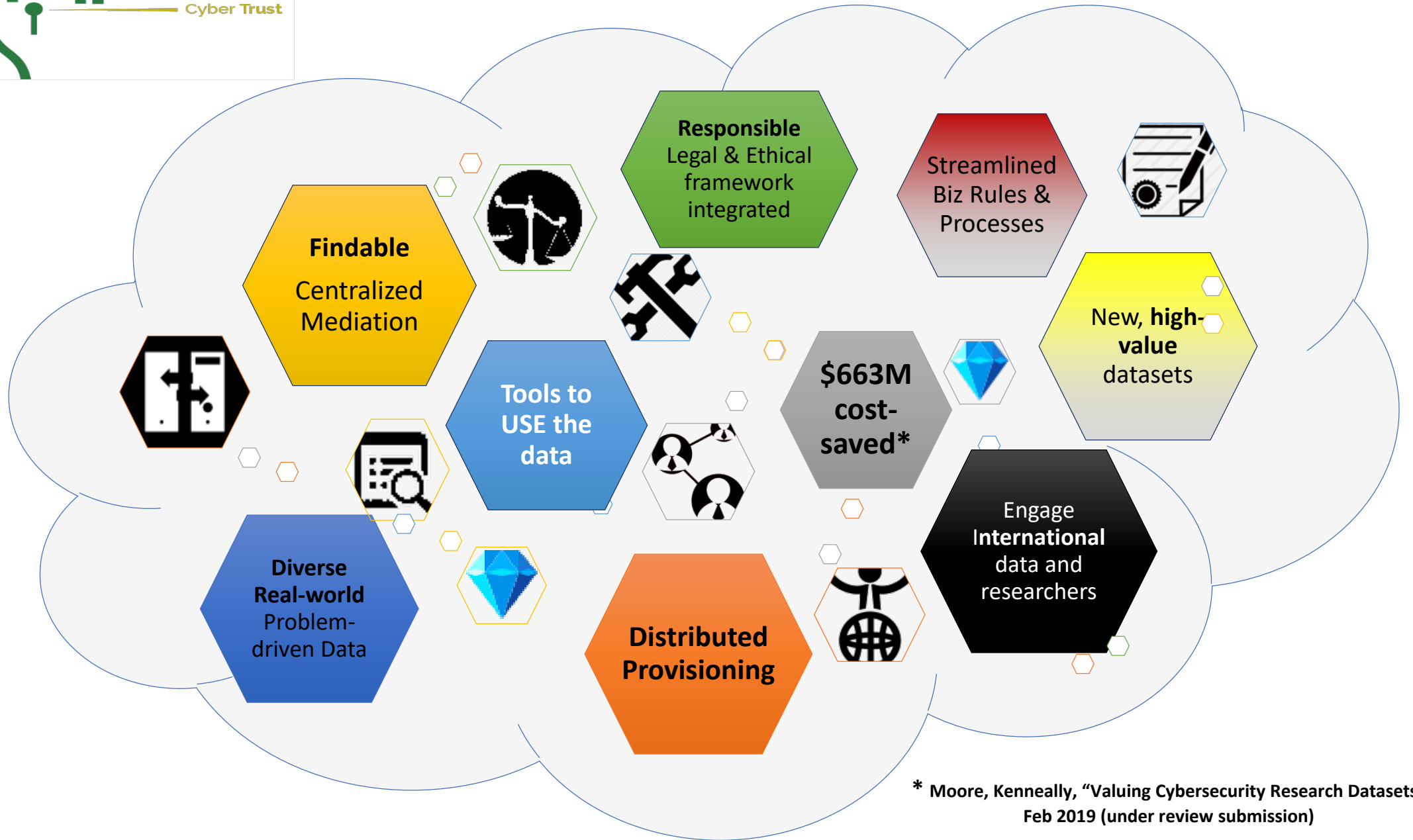
New Zealand, Ireland, Spain, Sweden, Germany, South Africa, Denmark, South Korea all eager to participate.

Metrics - Top 10 Countries (December 2017 - April 2018)

Country	Sessions	Sessions	Contribution to total: Sessions
	6,847 % of Total: 100.00% (6,847)	6,847 % of Total: 100.00% (6,847)	
1. United States	3,495	51.04%	
2. China	448	6.54%	
3. India	346	5.05%	
4. United Kingdom	229	3.34%	
5. Israel	212	3.10%	
6. Taiwan	159	2.32%	
7. Canada	146	2.13%	
8. Singapore	130	1.90%	
9. Spain	125	1.83%	
10. Australia	116	1.69%	

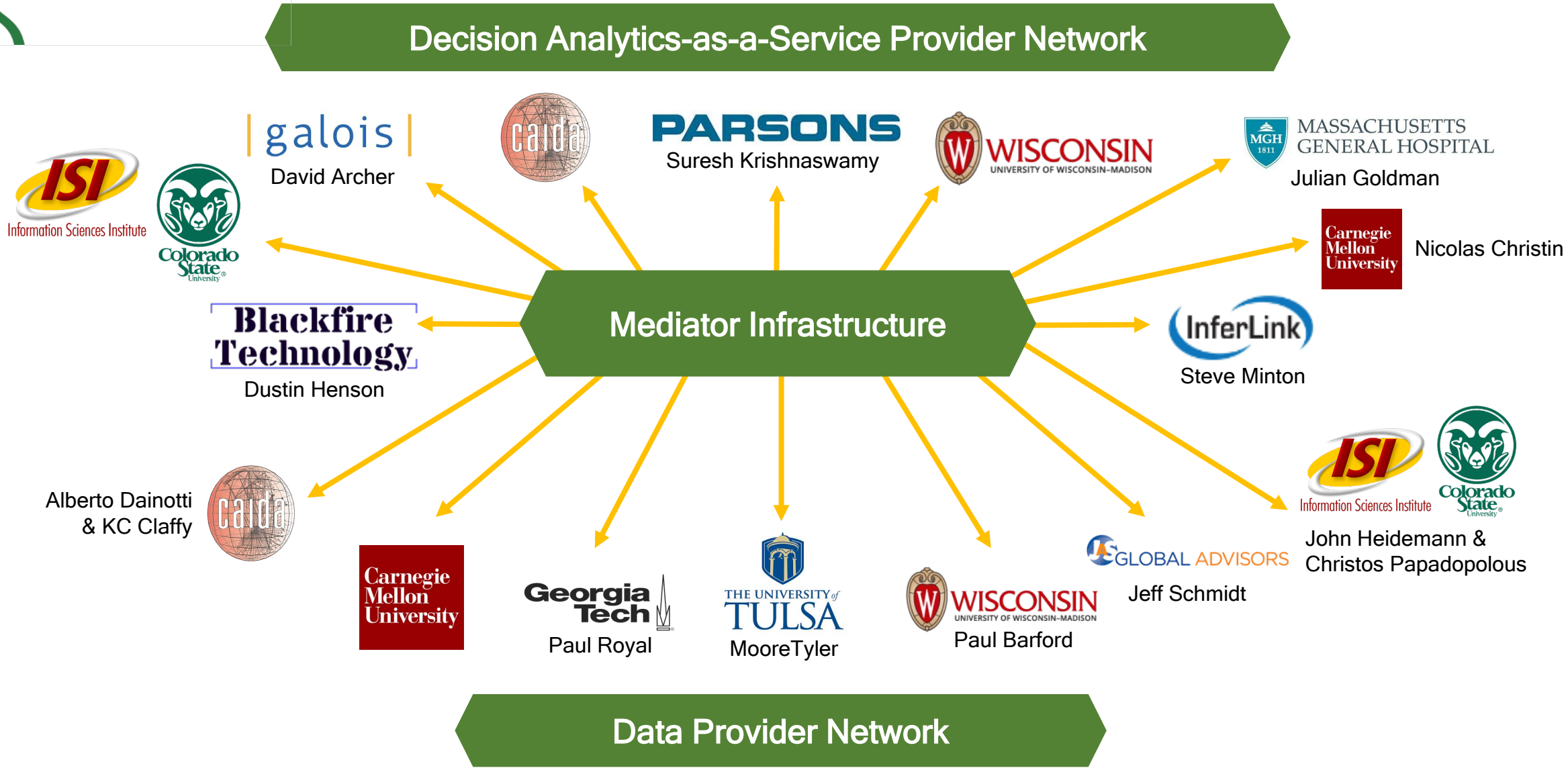


Success Elements

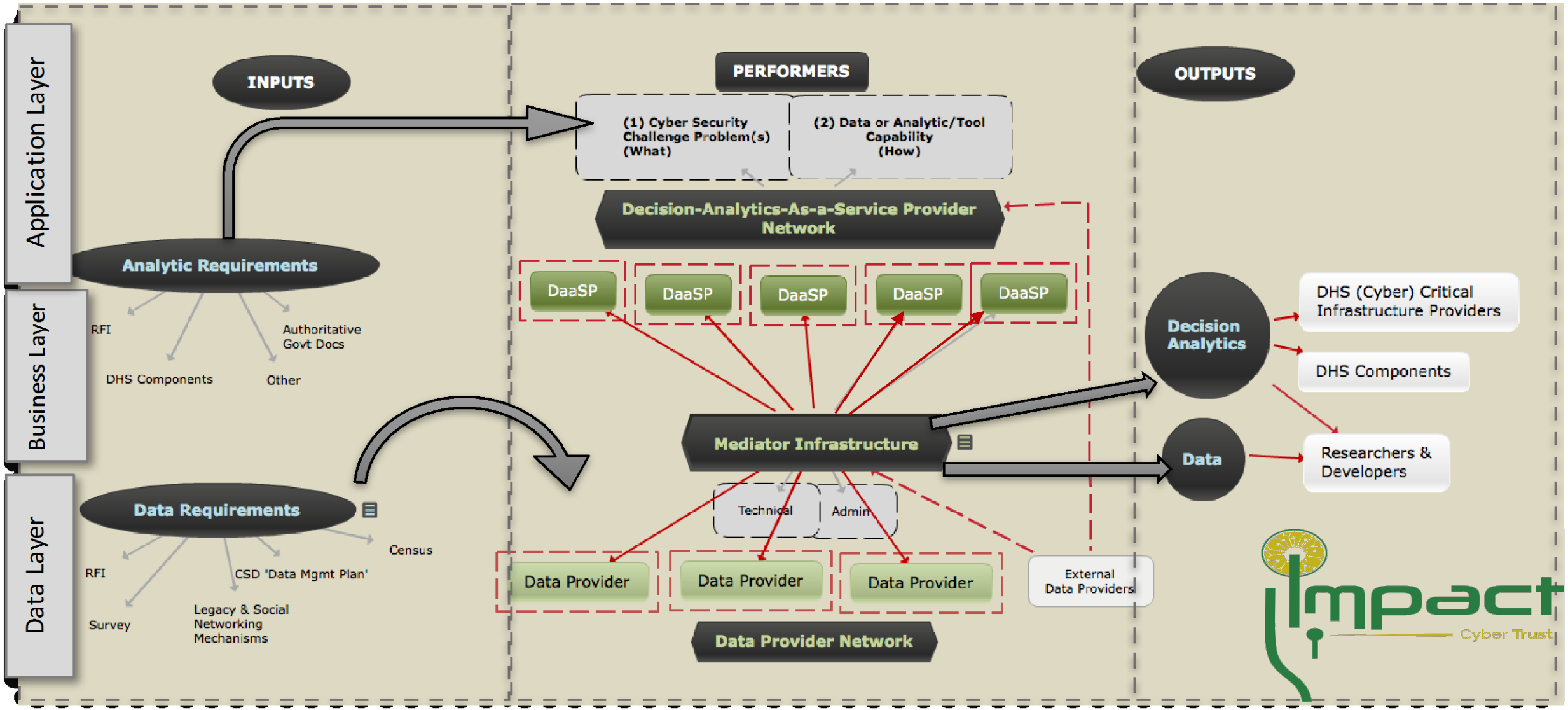


* Moore, Kenneally, "Valuing Cybersecurity Research Datasets" Feb 2019 (under review submission)

Current Booths in the Marketplace



Evolved Model Recap



Booths and Wares in the Marketplace:

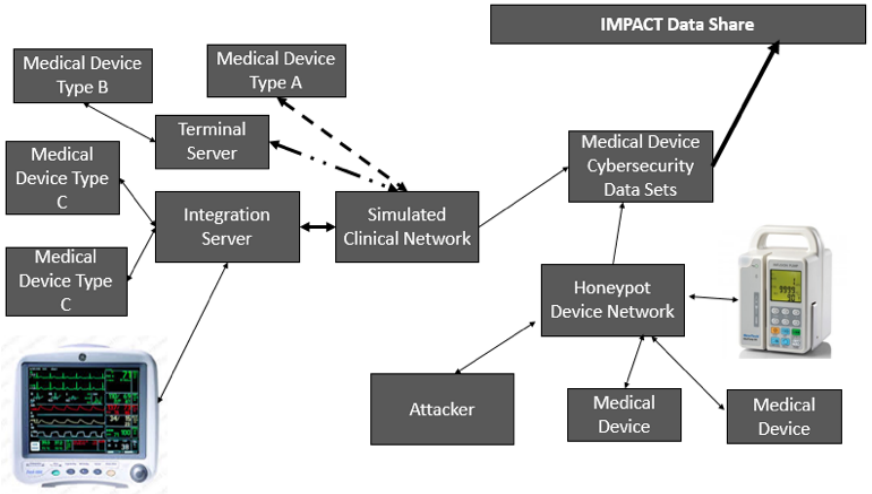
Information Sciences Institute

Colorado State University

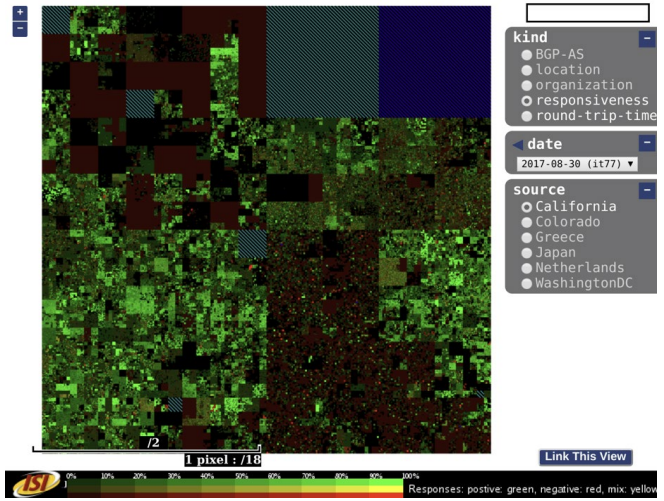
PARSONS

MASSACHUSETTS GENERAL HOSPITAL

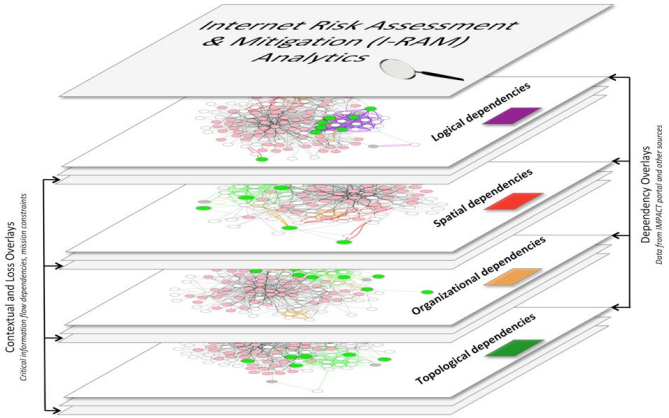
One of the world's only medical device lab datasets: network honeypot & simulated hospital scanning & attack data



Longitudinal data: anonymized packet headers and netflow data, Internet censuses and surveys for IPv4, Internet hitlists to drive topology studies, Internet outage observations, and DNS and IoT application data

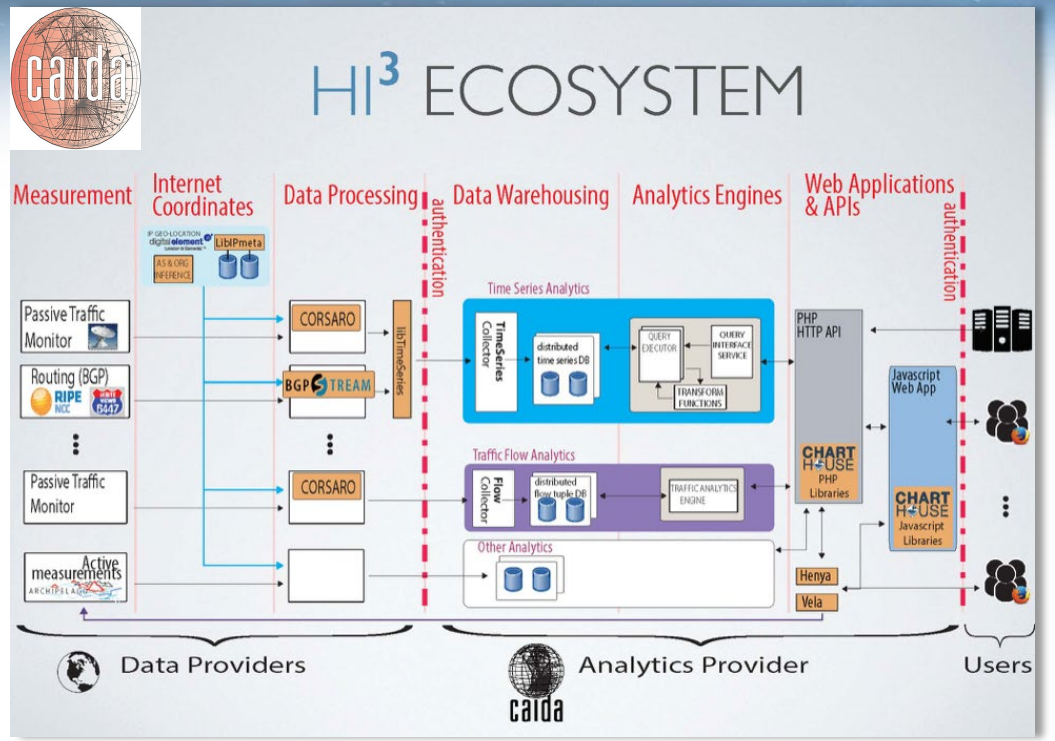


Enterprise–level Internet Exposure Risk model and metrics: Aggregate measures to help assess an org's dependencies on the Internet infrastructure



Impact Cyber Trust

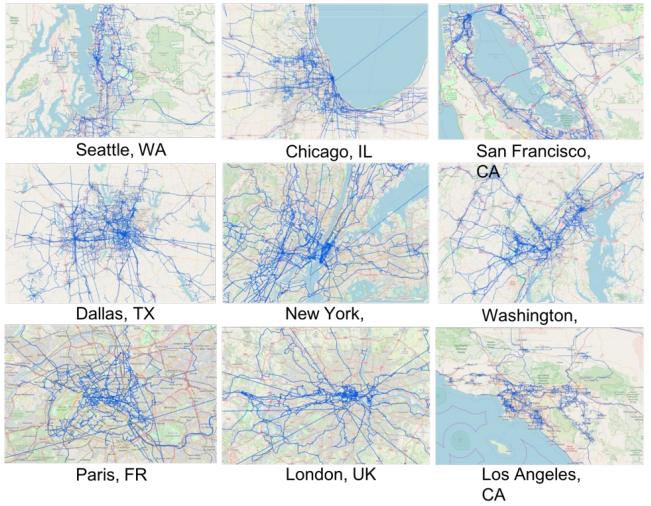
Booths and Wares in the Marketplace:



Fuse, correlate, x-validate multiple streams of historical and real-time Internet measurement (IP, BGP, topology/AS, darknet, geo-political coord, DNS, WHOIS) enabling informed ID and response to attacks and other disruptive events.

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

Internet Atlas- physical internet infrastructure maps, which includes nodes (e.g., hosting facilities and data centers), conduits/links that connect these nodes, and relevant meta data (e.g., source provenance).

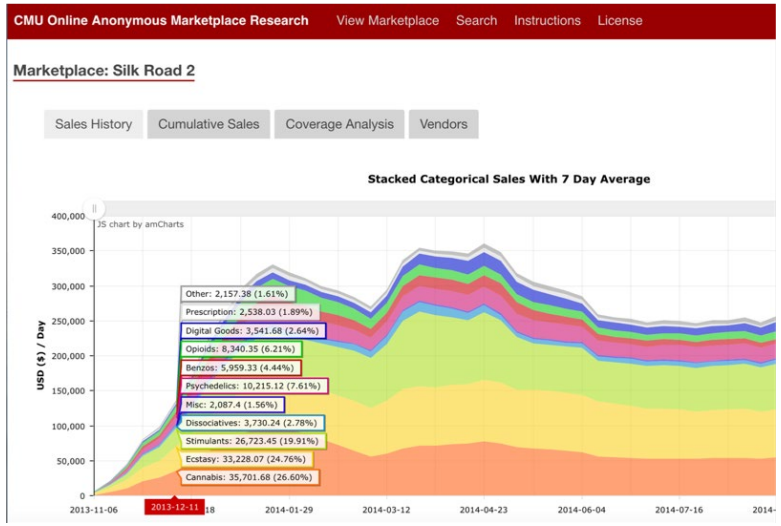


Impact Cyber Trust

Booths and Wares in the Marketplace:

Carnegie Mellon University

Continuously monitoring largest online anonymous "darkweb" marketplaces. Measurements help researchers better understand how online criminal threats operate & evolve over time.

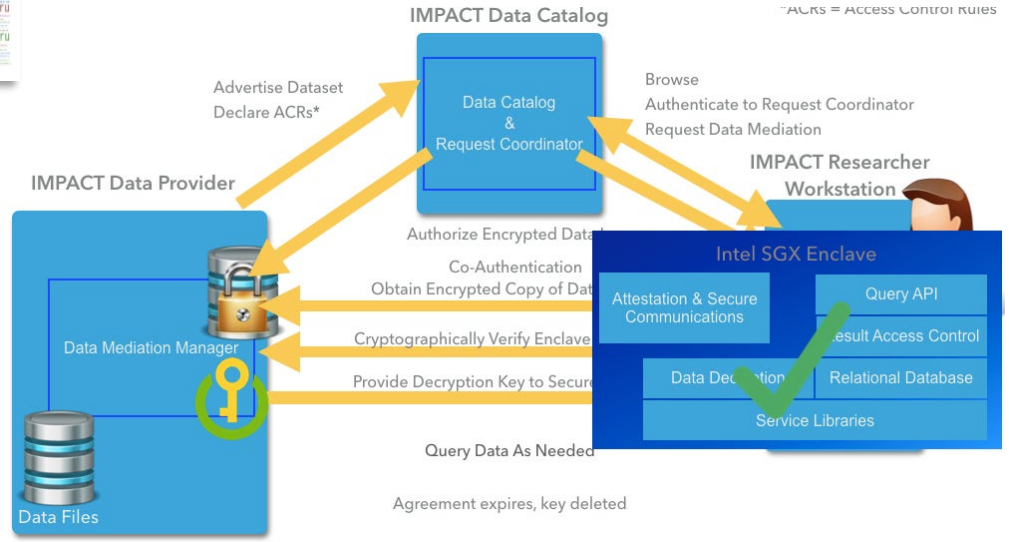


Georgia Tech

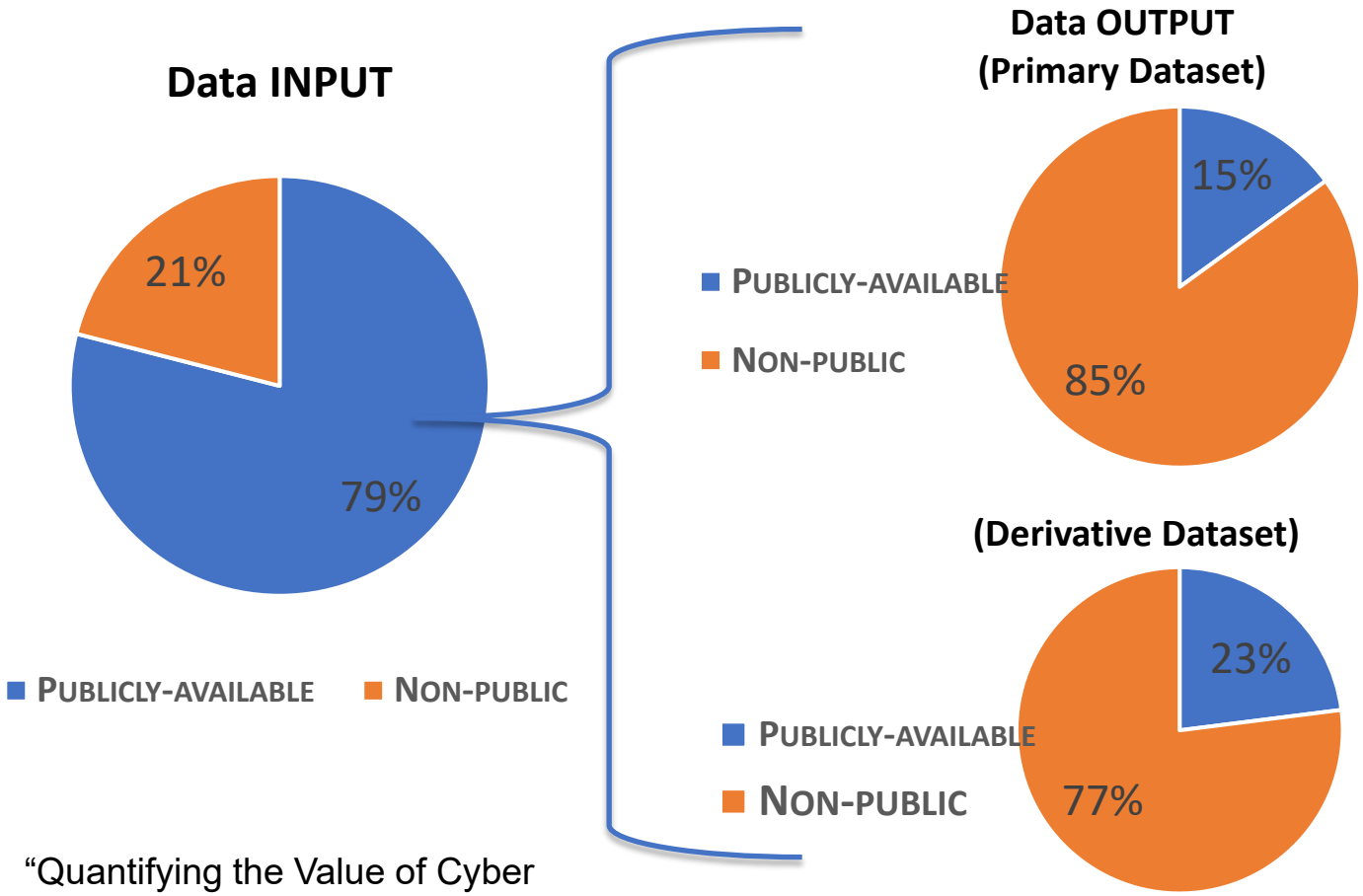
Network- and host-level malware datasets for research and/or operational use, to individuals and organizations for whom this data would otherwise be inaccessible.

galois

FIDES is a technical disclosure control system for enabling data utility and protecting sensitivities. Keeps non-anon sensitive data cryptographically secure for lifetime.

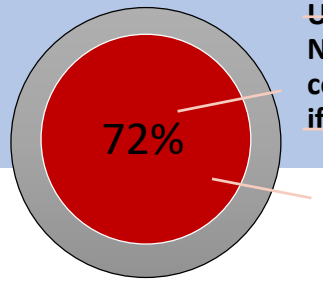


Do We Have a Problem?



"Quantifying the Value of Cyber Security Data Sharing for R&D"
Tyler Moore, U. of Tulsa

- **Public Datasets valuable, but under-provisioned**
  - Demand >>>>> Supply
- **Value Incentives:**
  Quantifying value of a public good is hard, particularly in $ terms
- Supply Side: Quantified, rational benefit
  - > pub cites
  - How to motivate Industry?
- Demand Side:
  - Myriad uses for data do not easily translate into $
  - Avoided Cost: **$663M** (since '06)
  - ?? Relationship $data provision :: customer demand

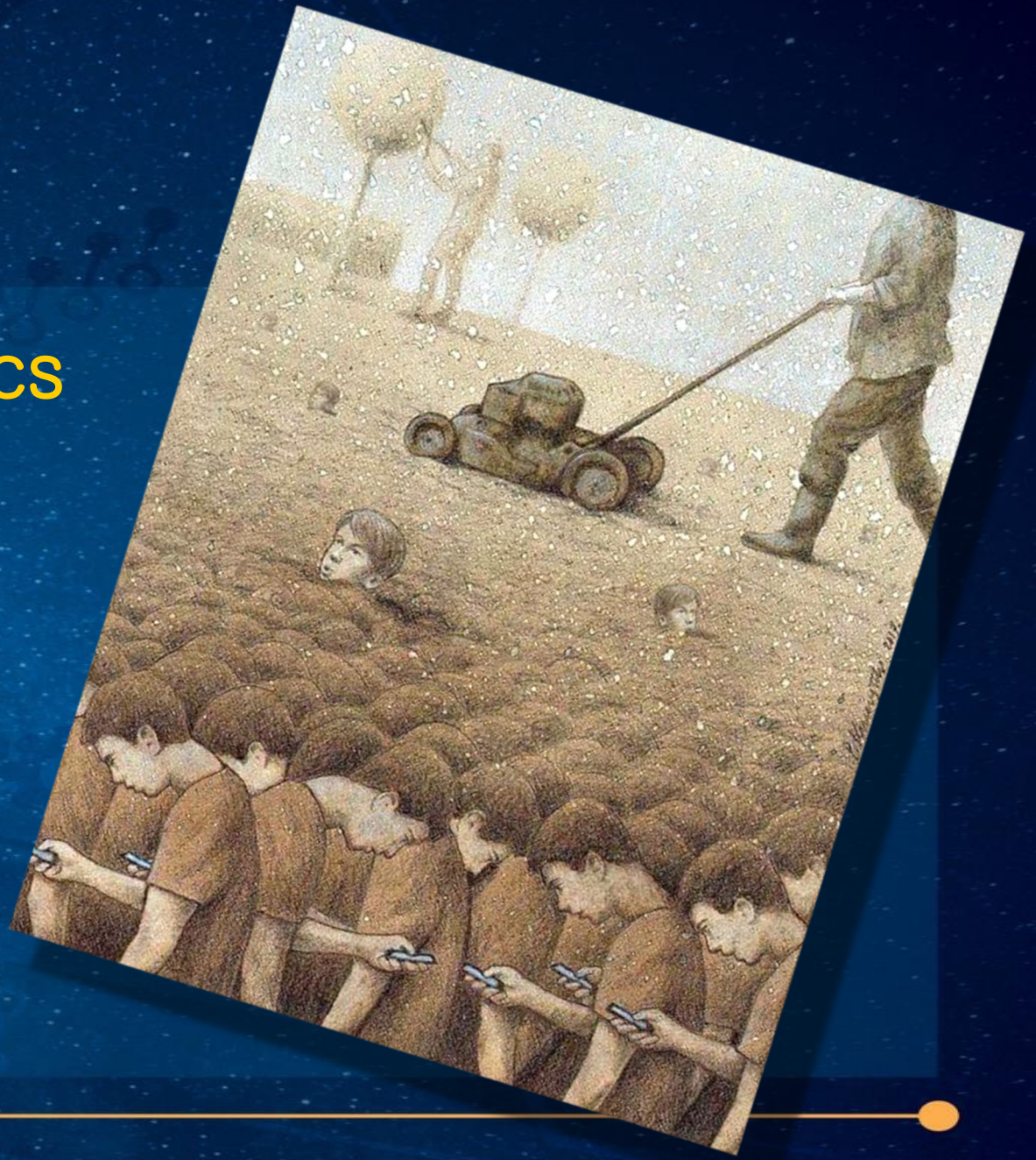


Users would NOT have collected data if no IMPACT

Transition Strategy

- Continue to expand Resource Provisioning to all cybersecurity stakeholders
- Scale and enhance integration with CISA data input and output needs
- Implement multi & bilateral international provisioning
- Expand International footprint to match demand
- Operationalize Public-Private Sector Model

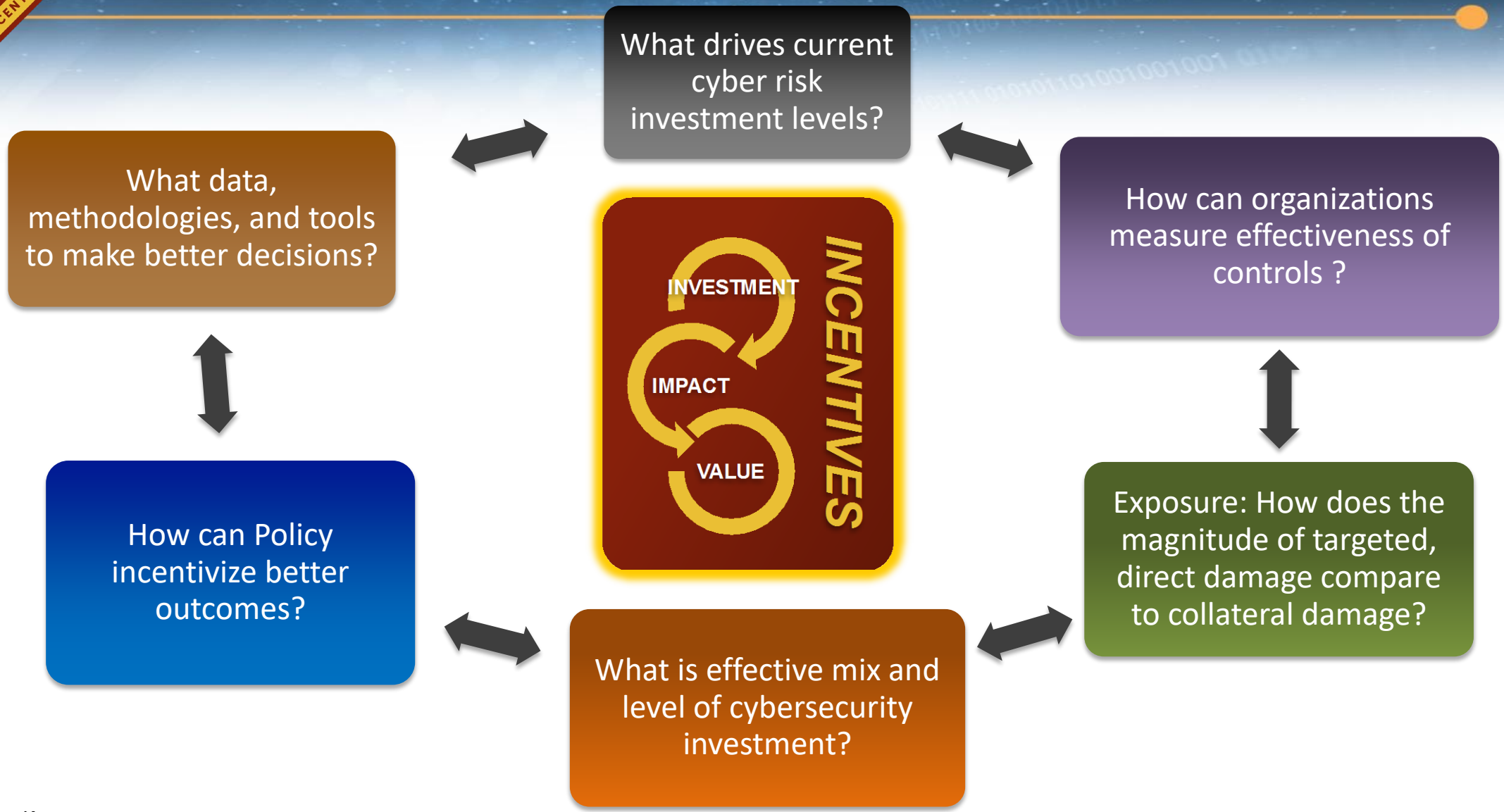
Mind :: Economics



Homeland Security

Science and Technology

Cyber Risk Economics: So Many Q's, So Few A's



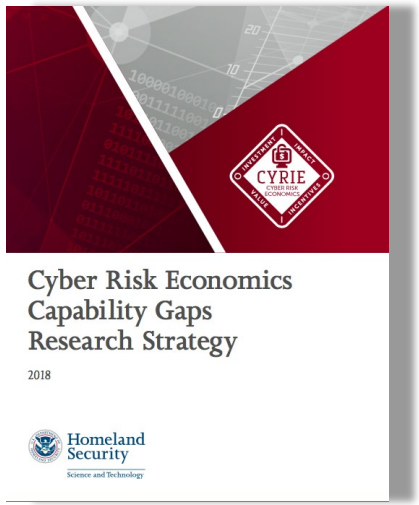
CYRIE Program Execution

Coordinate & Convene

- Stakeholders: USG, industry, researchers
- Stakeholder Exchange Meeting (SEM) (2/17)
  - Addressed capability gaps, practices, economic behavior, and research challenges
- SEM 2 (9/17)
  - Addressed targeted capability gaps and research objectives
- SEM 3 (6/18)
  - Economics of IoT Security
- SEM 4 (4/10)
  - Economics of Internet Infrastructure Security

Knowledge Products

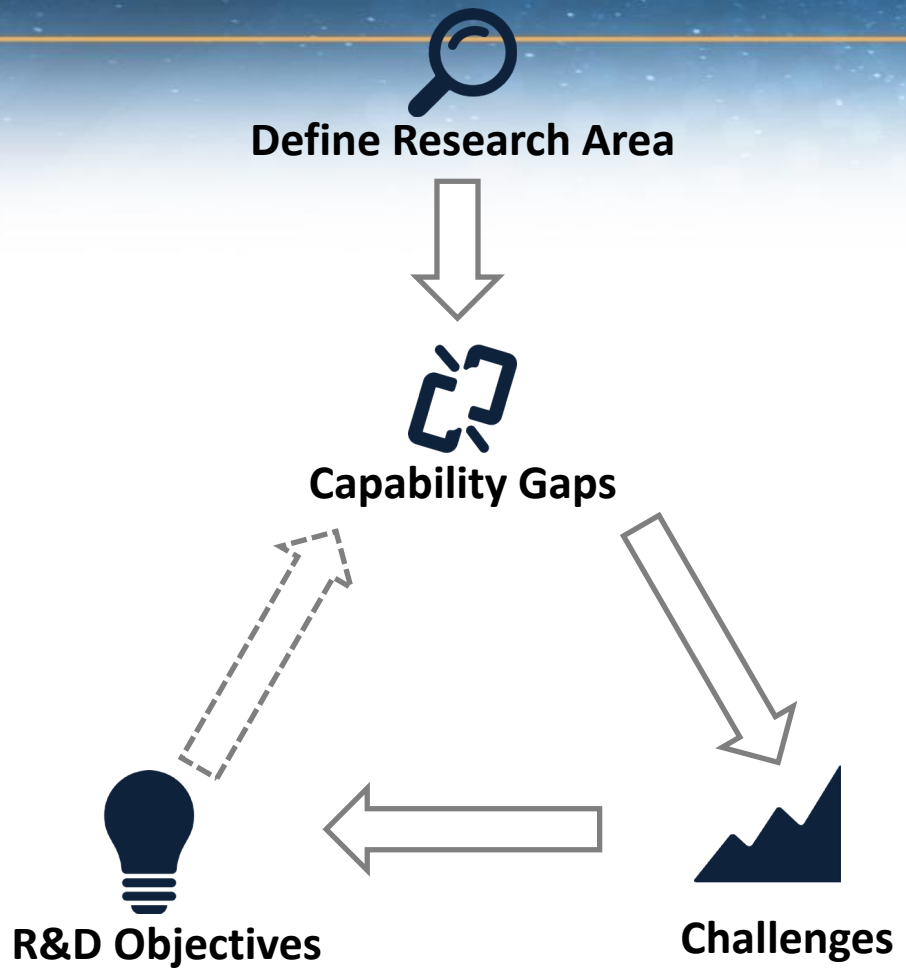
- Cyber Risk Economics Capabilities Gaps Research Strategy, published (October 2018)



Applied Research & Advanced Development

Fund Technologies, Models, Metrics that address the business, legal, technical, and behavioral aspects of the economics of cyber risk relative to cyber threats, vulnerabilities, attacks, and controls.

Cyber Risk Economics R&D Strategy



THEME 1 – Quantification of Risk
Area 1 – Entity Risk Assessment Area 2 – Systemic Risk Assessment Area 3 – Impact of Controls Area 4 – Decision Support
THEME 2 – Role of Government, Law, and Insurance
Area 5 – Role of Government Regulation Area 6 – Role of Insurance Area 7 – Role of Law and Liability
THEME 3 – Third Party Risk
Area 8 – Supply Chain Accountability
THEME 4 – Organizational Effectiveness
Area 9 – Organizational Effectiveness
THEME 5 – Data Collection and Sharing
Area 10 – Information Asymmetries Area 11 – Data Collection and Mapping
THEME 6 – Threat Dynamics
Area 12 –Adversary Behavior & Ecosystem

DHS.gov/publication/Cyrie-Capability-Gaps-Research-Strategy

Cyber Risk Quantification

Area 1 – Entity Risk Assessment

- Fundamental challenge: **lack of cyber exposure understanding**
- **RA 1.0** = Breaches proxy risk
  - #rcrds, data type, source, and use
  - Ex-post, descriptive
- **RA 2.0** = External signals (blind spots)
  - Misconfigurations, malicious activity, and security incidents
  - Ex-ante, forecastive
- **Not incentivized** to disclose risk- and impact-related data
- Inherently **hard-to-measure** and hidden nature
  - Insiders; 3rd party, reputation, and geographic

- RA 3.0 = More complete risk (nature, size, frequency, impact) along **granular attributes**
  - 3rd parties, online footprint, information value, code complexity, and Internet exposures based on dependencies (protocols, services, info, and affiliations)
- Evaluate how **magnitude** of risk varies by source of risk (e.g., attackers, malicious insiders, negligent practices, systems and technical failures, and internal process failures)

Cyber Risk Quantification

Area 2 – Systemic Risk Assessment

- **Insufficient data and knowledge**
  Frequency, impact, distro of cyber risk on critical infrastructure and across industries
  - Improvement at host level but little understanding of how to roll this up to macroscopic risk level
  - Cost estimates variance ($B-$T)
- **Identifying diversity in dynamic threat, interdependent, and correlated risk ecosystem**
  - Cloud Down Report
  - NotPetya Maersk, Dyn
  - Likely concentration of risk in SMB → behavior and controls investment harder to measure

- **Exposures models and data:**
  Seams, Adoption, Dependencies, Automation
  - Efficiencies → Functional Interdependencies → Aggregated Risk → Systemic/Cascading Harm
  - Impacts of cascading effects across critical infrastructures
- Normalize common **lexicon**, methodologies, and data dependencies

Risk Quantification → Impact of Controls on Risk

Area 3 – Impact of Controls

- **Oracles are failing us**
  ~15% market growth; $T spend forecast
- **Poor Correlation Risk → Controls**
  - Standard benchmarks hard to measure, breach non-disclosure, audits point-in-time, multi-vendor tenancy, upgrade resistance
- **Ditto Controls → Harm**
  - Economic losses: direct and indirect, lost time, and productivity
  - Data compromise
  - Reputation damage
  - Privacy liability
  - Remediation and protection measures
  - Trust loss and social instability
  - Damage to physical systems and critical infrastructure

Data that maps specific cybersecurity controls **experience :: outcomes**

- **Hard risk controls :: soft risk** controls (policy, training, and best practice)
- Develop **value- and outcome-based** measures and metrics for assessing efficacy of technical controls
- **Human v. Tech**: where can security be automated v. human in the loop

Third Party Risk

Area 8 – Supply Chain Accountability

- **Accountability** for vulnerabilities and breaches within complex supply chains, product/service pipeline
- Manufacturers lack **tools** to account for cyber risk introduced by component technology
- Legal/regulatory framework challenged to assign **transitive responsibility**
- IoT security **market failure**?
  - Scale and diversity of vendors
  - Incentives to compete on $$ and not security
  - < Incentive to coordinate security efforts

- **Model incentives** and mechanisms for upstream and downstream suppliers to cooperate to improve cybersecurity
- How exposure to **liability** changes behavior, investment and outcomes
- Develop mechanisms to correct or mitigate **information asymmetry** in the supply chain
  - Model bill of materials
  - Audit capability to enable manufacturers to certify components and choose suppliers (MUD)

Program Execution: Technologies, Models, Metrics

FOURSight: An Information Market to Crowdsource & Gamify Defense

Need

- Understand **empirical and experimental** effectiveness of cybersecurity controls
- **Unbiased resource** to assess tech investments and gauge performance (peers and best practices)
- **Incentivize sharing** and aggregation of forecasts to improve defense

Approach

- Operationalize **crowdsourcing** to evaluate controls via game forecasting
- **"Bug Bounty"** for breach controls efficacy
- Create **market** in defensive playbooks against emerging threats to accelerate security innovation

Benefits

- **Talent-spot** best analysts; train to reduce cognitive bias
- Inform **automated methods** to reduce cyberattack impacts and risks

PI Mark Jaster

Cyber Risk Econ Applied: Incentivizing Data

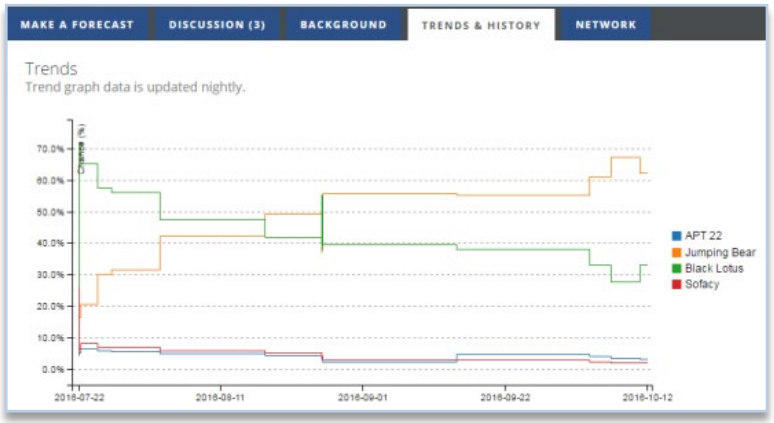
Get Points

Analyze Incidents, Data or Cyber Intel

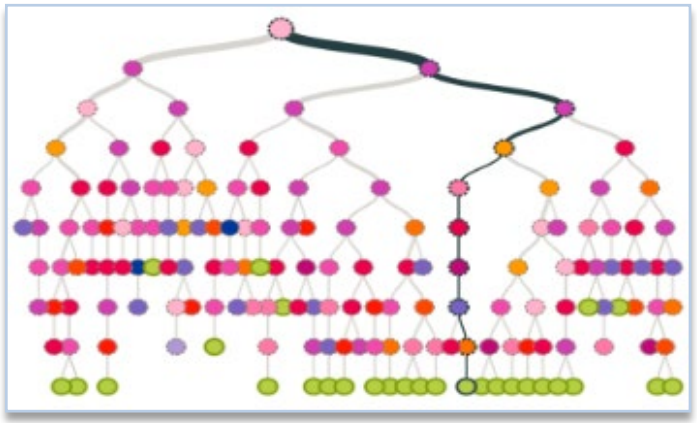
Bet Outcome Probabilities

Get Payouts & Recognition

Threats & Controls Efficacy Trends



Predictions & Inferences



CYRIE
CYBER RISK ECONOMICS
INVESTMENT
IMPACT
VALUE
INCENTIVES

"FOURSight: an Information Marketplace to Crowdsource Cyber Controls" 418 Intelligence

Quantifying the Value of Cybersecurity Data Sharing for R&D

Need

- **How is data being produced and used** by researchers, what data is being shared, and what is not
- **Improve availability** of valuable measurements and analyses that remain bottled up
- Goal - **identify economic underpinnings** and incentives for greater sharing for cybersecurity

Approach

- Census of top technical cybersecurity publications and **documenting data inputs, outputs, and outcomes**
- **Analysis of ~2,300 IMPACT data requests & Cost to share**

Benefits

- 72% surveyed would not have collected the data themselves if it wasn't available in IMPACT
- **$663 million (total value since 2006)**

Median cost to provision

Category	Cost
# Personnel	3
PI	$38,500
Software Developer	$87,000
System Administrator	$80,000
Research Staff	$30,825
Managerial Cost	$37,000
Equipment	$18,250
Total	**$291,575**

PI Tyler Moore, U. of Tulsa

Standard Model for the Costs of Cybersecurity Attacks

Need

- Open, data-driven model to **understand harms to victims from malware attacks**
- Translate attack incidence into attack harm by estimating the distro of severity across different infections by different strains of malware / across different cybercriminal campaigns

Approach

Cyber Attack INCIDENCE X **Cyber Attack SEVERITY**

Available from vendor telemetry, passive dns, botnet infiltration, etc

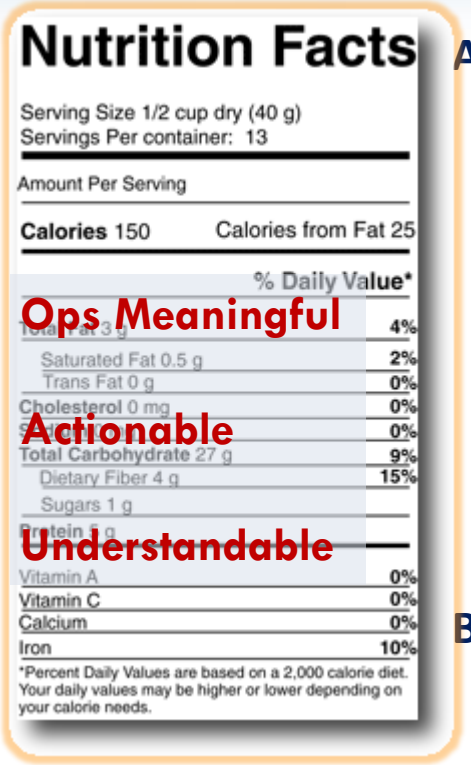
Macro level: passive measures of infection details, remediation, harms
Micro level: active investigation of individual events

Benefits

- Identify, prioritize, evaluate risk exposure, liability, and hard and soft controls gaps
- Translate future attacks into harm metrics ($$$/time) with a **standardized, open** methodology

Kanich, U. Illinois Chicago

Foundations of Threat Intelligence Metrics



Need

- Normalize, compare, and assess the **reliability of cybersecurity threat indicators**

Approach

- **Threat intelligence metrics:**
  - Technical- accuracy, coverage, timeliness
  - Comparative- intersection, uniqueness
  - Risk- successful, attempted attacks
  - Collateral Damage- adverse effects of FP (eg, auto block a harmless domain)
  - Operational- how tech metrics work in the org (eg, feed TP rate)

Benefits

- **TI Reliability Score:** improve automated defenses, threat analysis, incident analysis, risk profiling

PI Levchenko, U California San Diego

Outcome-Based Cybersecurity Risk Management

Need

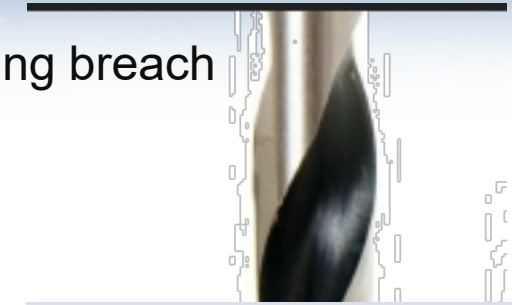
- Little cyber risk management is **outcome-based** (security investment :: resulting breach risk)
- Firms cannot answer **basic questions**
  - How much security is gained from investing in certain controls?
  - What controls reduce risk?

Approach

- Empirical **data: Internal Enterprise & End-Users, External firms**
- Predictive **models** on causal links between behavior & outcomes

Benefits

- Better manage cyber risk viz **causal links** between controls → security level → outcomes
- Metrics & findings incorporated into 3 partner security firm's products



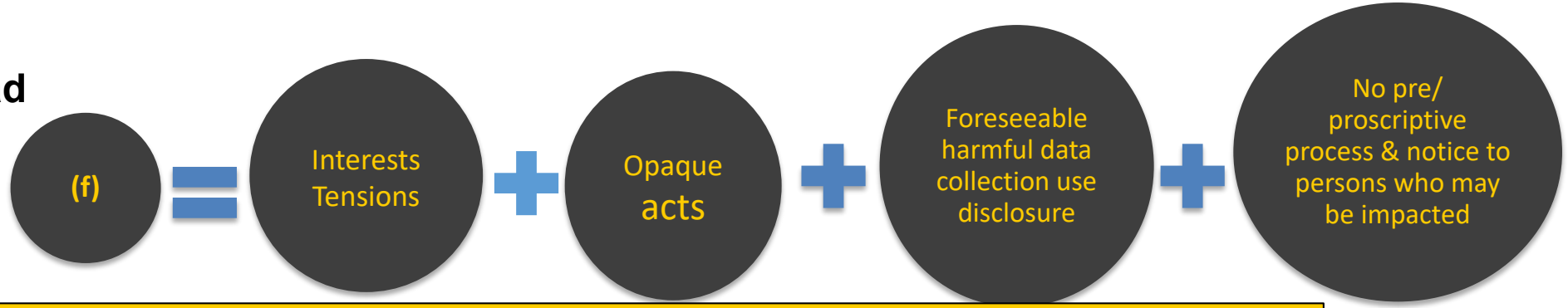
"People do not want a ¼" drill, They want a ¼" hole"

Moore- U. Tulsa; Christin- CMU; VanEeten, Delft U.

Spirit :: Ethics

- **Which involves anonymous observation, collection, and use of sensitive data in Smart Communities w/o interacting with the data subject?**
  - (a) Cyber espionage and surveillance by industry or nation-states
  - (b) Advertising and data brokering by industry
  - (c) Targeted services and content by vendors
  - (d) Monitoring by Govt (stingrays, “public” data)
  - (e) Security R&D
  - (f) All of the Above

- **Common Thread**



- **How to differentiate between these acts & actors / What’s “right v. wrong”?**
  - When law on “harm” is silent/unclear/gaps?
  - When tech is *quintuple-purpose*?

Ethics Implementation Options

- **(1)** "Ethically-Defensible" Research & Commerce
  - **Tool Building**: Decision support capabilities, Notice & Consent, Disclosure Control
    - **Education & awareness**
    - **Self Governance**; community consensus & oversight; market differentiation
    - **Enlist expertise**

- **(2)** Stick/Carrot :
  - Dreaded **"R"; xRBs**
  - **Tie to funding**, publication; reward ethical behavior
- **(3)** Getting *New York-Times'd*
  - **Reputation** lever

CREDS

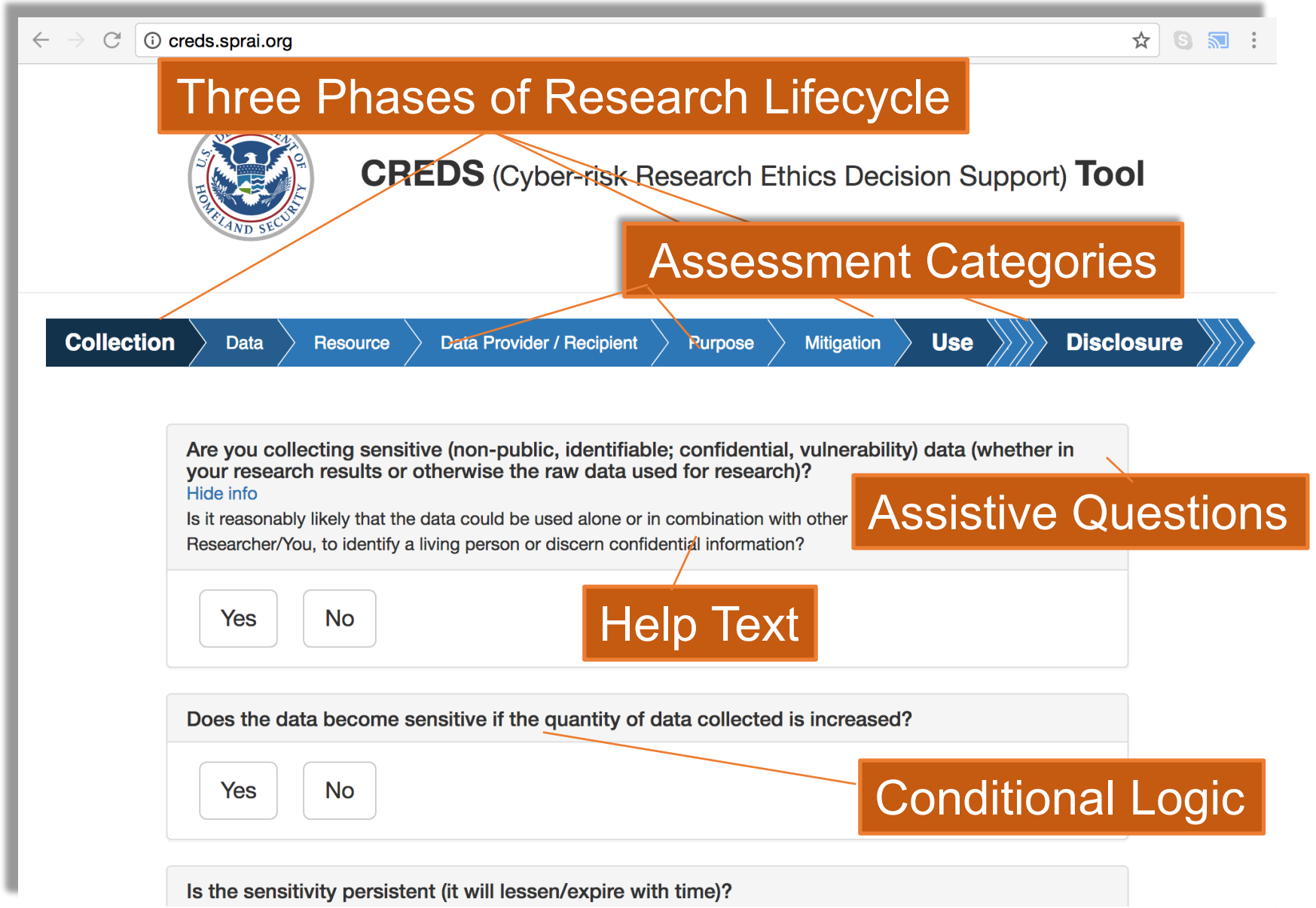
CREDS Tool – Ethics Logic

ETHICAL IMPACT ASSESSMENT

Research Lifecycle	Ethical Principles	Risk Factors	Assistive Questions
(1) Research Collection (2) Research Use & Management (3) Research Disclosure	**Respect for Persons -** (Identification of	**Nature of the Data**	
		Sensitivity: non-public, identifiable; confidential	
	Beneficence (Minimizing risk to individuals; Maximizing benefit to society; Mitigating realized harms))		
		Nature of the Resource/System	
		Platform	
		Network	
		Nature of the Data Provider, Data Recipient, Data Subject	
		Stakeholders rights and interests	
		Nature of the Data Collection Purpose	
	Justice (Fairness & Equity in selection of subjects and distribution of research benefits)	**Harm Mitigation**	
	Respect for Law and Public Interest (Compliance with Law; Transparency & accountability of actions)	Collection controls (operational (access type), data (filtering, anon), legal/policy agreements))	
		Data Protection	
		Stakeholder consent	
		Legal Exception	

(1) (2) (3)

CREDS Tool – Operationalizing Ethics



Kenneally

CREDS Tool – Ethics Risk Heat Map

CREDS (Cyber-risk Research Ethics Decision Support) Tool

Heatmap

Results Summary

	Data	Resource	Data Provider/Recipient	Purpose	Mitigation
Collection	4 / 9	1 / 2	1 / 2	1 / 3	3 / 5
Use	1 / 2	3 / 5	2 / 3	4 / 8	5 / 9
Disclosure	7 / 13	1 / 1	2 / 4	0 / 0	0 / 0

Detailed Q&A Breakdown

Lifecycle	Risk Factor	Question	Response
Collection	Data	Are you collecting sensitive vulnerability) data (whether i data used for research)?	No
		Does the data become sensitive if the quantity of data collected is increased?	Yes
		Is the sensitivity persistent (it will lessen/expire with time)?	No

…and then there's the AI Cybersecurity Challenges

Governance

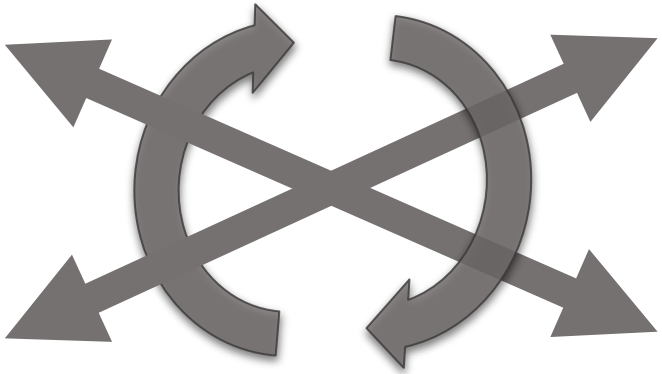
- **Standards** for safe responsible data, AI
- **Privacy** sensitive models
- **Liability** regime

Risk Understanding & Unintended Consequences

- **Skewed risk posture** → false +/- generalizable, accuracy
- Cyber security **not well-defined problem** for AI: Dynamic code, attack surface, adaption methods

Data Deficiencies

- Massive labeled realistic **training sets**
- Not **purpose-driven**



Ethics, Values, Rights, Interests

- Principles, applications, enforcement
- Tech becoming decision-maker; **impact** on people, org **autonomy**, trust?

Augmented Control

- **Trigger** for human-in-the-loop?
- **Explainability**: AI, data & model transparency

Advanced Analytics & Autonomous systems

- **Bias/fairness** in both D&A – guise scientific, proprietary
- **Resolutions** not all binary Rt v. Wrong → judgments, values

Trusted Innovation.

Erin Kenneally, M.F.S., J.D.

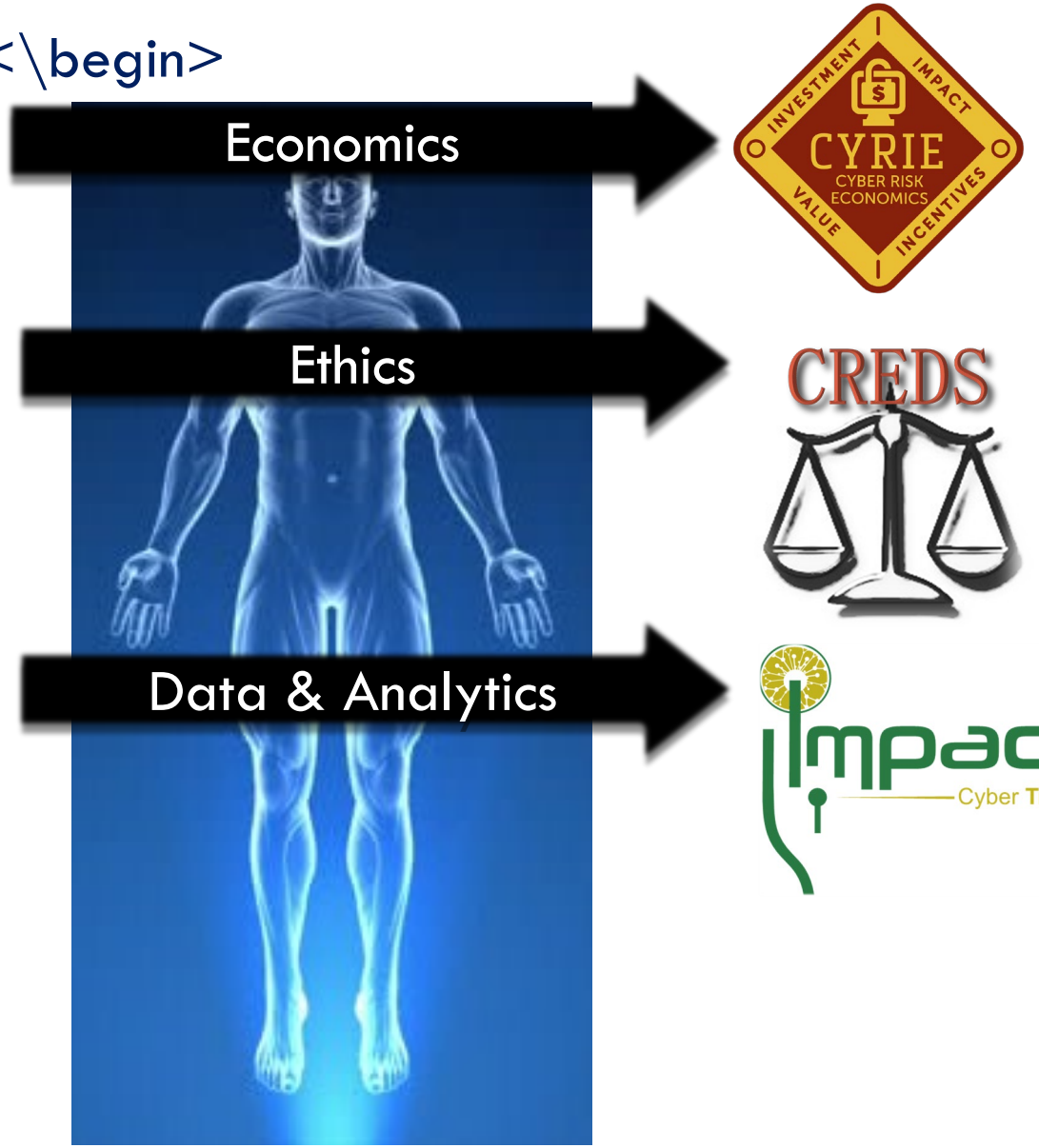
Cyber & Physical Security Division

Science & Technology Directorate

Dept of Homeland Security

Erin.Kenneally@HQ.DHS.Gov

<\begin>



<\end>