



POWERED BY
BOUNDLESS COLLABORATION.
COMMUNITY
CONNECTED RESEARCH. ACCELERATED DISCOVERY.

www.internet2.edu  [@internet2](https://twitter.com/internet2)

KINBERCON 2017: Cultivating Smart and Connected Communities

PRESENTED BY: Florence D. Hudson, Senior VP and Chief Innovation Officer, Internet2

Internet2 – Not for Profit, Member-Owned Consortium.



Network Services – 100 Gbps network

Trust & Identity – Federated Identity Management

Cloud Services (NET+) – 30 cloud services available

Community Engagement – 500+ members in Higher Education, Regional Networks, Industry & Affiliates

Innovation Office – Community-led innovations

US UCAN – 93,000 community anchor institutions



POWERED BY COMMUNITY

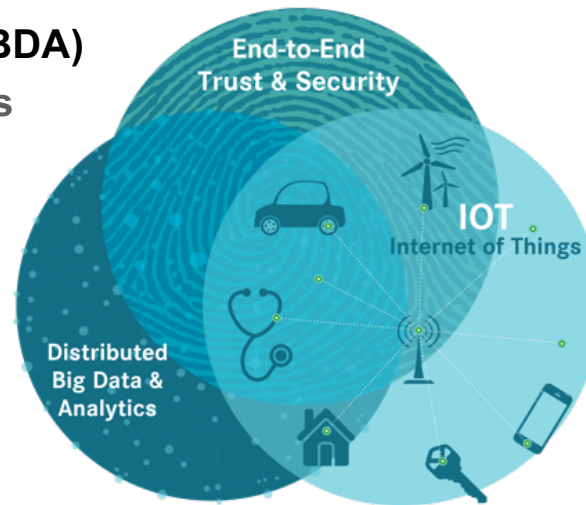
Internet2 Collaborative Innovation Community is the combination of three member-led innovation working groups, focused on areas related to our top two priorities of advanced networking plus trust & identity, including smart campus/cities.

E2E Trust & Security (E2ET&S)

- **TIPPSS for IoT – Trust, Identity, Privacy, Protection, Safety, Security**
- NSF EAGER Cybersecurity Transition to Practice Acceleration
- *SDP (Software Defined Perimeter), Network Segmentation for IoT*

Distributed Big Data & Analytics (DBDA)

- Health & Life Sciences / Genomics
- **Smart Campuses & Cities**
- NSF Big Data Hub Collaboration



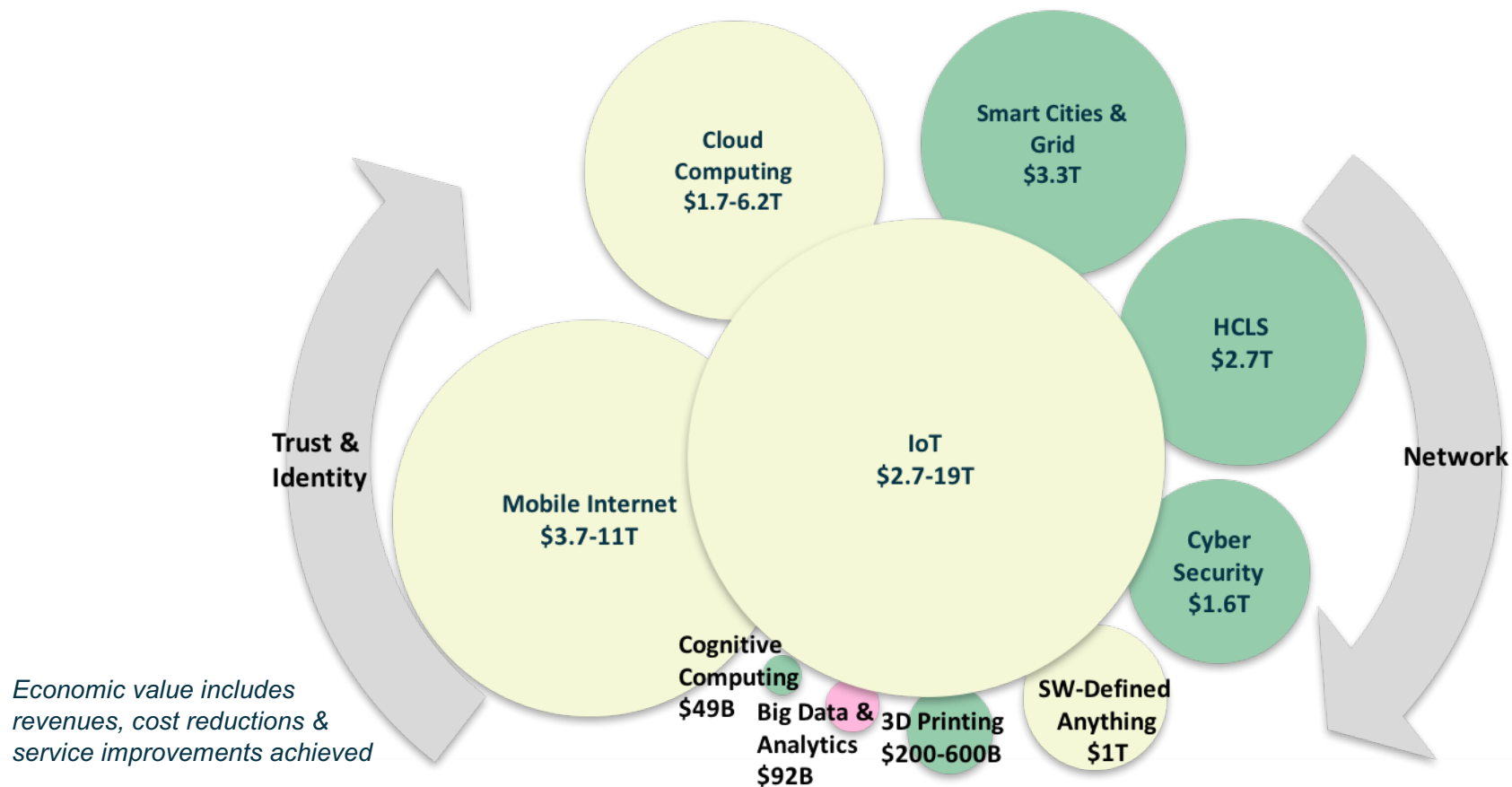
Internet of Things (IoT)

- IoT Sandbox
- **Smart Campuses & Cities**
- Smart Grid Testbed

Key:

Advanced Networking plus Trust & Identity
Advanced Networking focus only
Smart Campuses & Cities oriented

The Internet of Things could represent \$19T in economic value by 2025, a significant component of key ICT trends for Research & Education and Smart Communities.



POWERED BY COMMUNITY

Sources: McKinsey 2016; Frost & Sullivan 2016; CNBC 2016; Markets & Markets 2016; Morgan Stanley 2016; CMS Wire 2016; Business Wire 2016; Wikibon 2016; Yahoo! Finance 2017

Smart Campus Initiative created based on member input & innovation working group use cases, with kickoff meeting at Global Summit 2016.

- Share best practices and recommendations to deploy Smart Campus capabilities
- Guided by a Smart Campus CIO Advisory Council
- Commissioned IoT Systems Risk Management Task Force
- Convened with Microsoft first annual Campus Connections Summit, 140+ university attendees, Feb 2017



POWERED BY COMMUNITY

Research & Education activities are growing in Smart Campus / Communities, IoT, end-to-end trust & security, big data & analytics, Smart Grid.




Smart Campus operations & data analytics research



Advanced Networking / Cybersecurity Research



Smart Grid research



Smart Grid research network testbed




IoT Lab for Research and Pedagogy



Smart transportation / IoT ethics [research](#)



Smart Grid research



Smart Grid research and data sharing




IoT Security, Privacy & Ethics



Trust, Identity, Protection, Privacy, Safety, Security



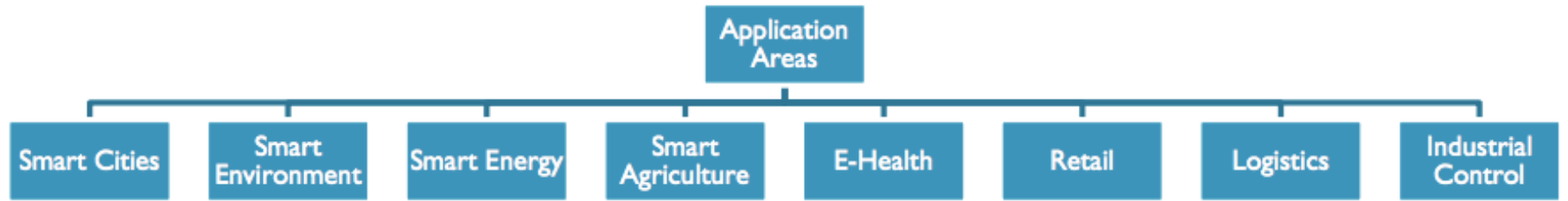
IoT Systems Risk Management & Security



[Smart Campus operations](#), trust and security

- Grey - IoT research and pedagogy
- Blue - IoT Smart grid research
- Orange - IoT security, privacy, ethics

ASU's View of a Smart Campus



Vehicle, asset, person & pet monitoring & controlling

Agriculture automation

Energy consumption

Security & surveillance

Building management

Embedded Mobile

Internet of things

Everyday things get connected for smarter tomorrow

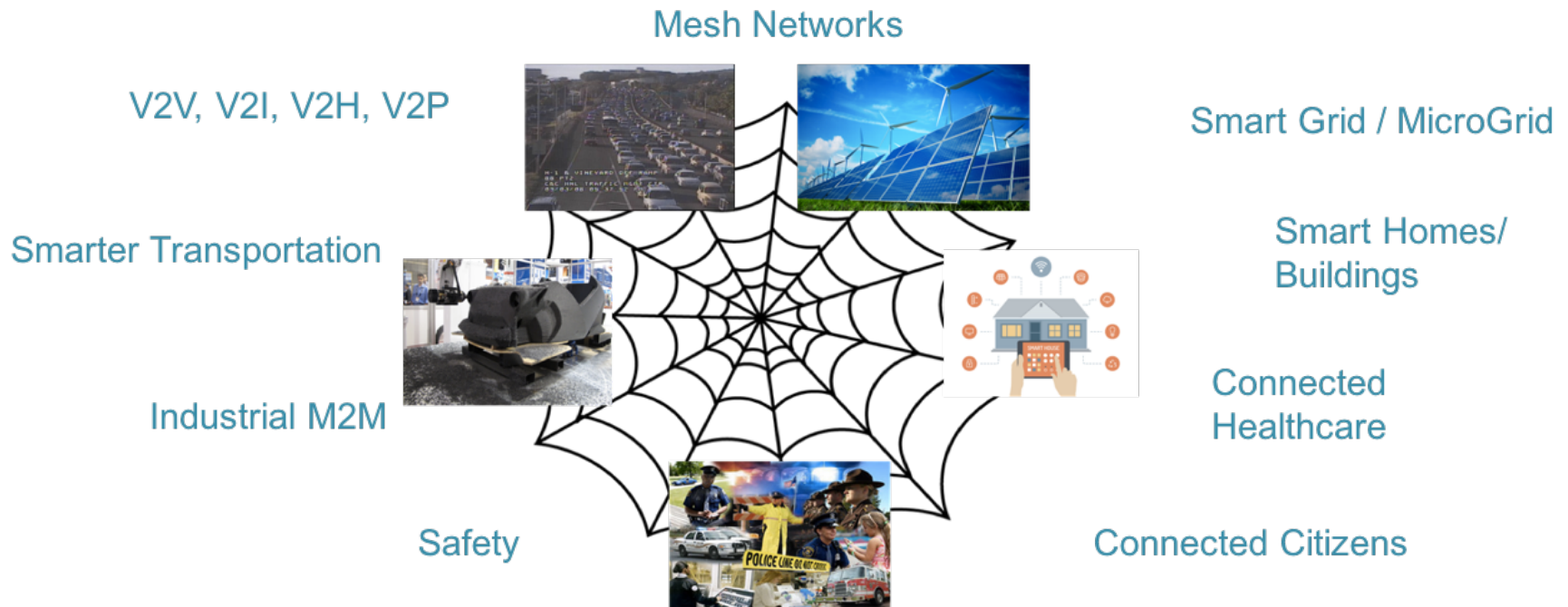
M2M & wireless sensor network

Everyday things

Smart homes & cities

Telemedicine & healthcare

Future smart communities will be an interconnected “system of systems” to improve efficiency, safety, quality of life, energy use, & environment.



What can we enable if we think across the system of systems?



POWERED BY COMMUNITY

February 2017 Microsoft Campus Connections Summit participants identified initiatives to further the Smart Campus journey.

- **Safety & Security**
 - Cybersecurity Learning Hub
 - Digital Literacy
- **Energy & Sustainability**
 - Campus as a Living Lab Breaking Cultural Barriers
 - Achieving Carbon Neutrality SCOPE ME
- **Success & Data Analytics**
 - The Agile University
 - Global Talent Profile
 - MentorBot Personal Tutor for Student Success
- **Collaborative Research**
 - Research Portal “1 Portal for All”

Internet2 IoT Systems Risk Management Task Force: Recommend Initial Exposure Benchmarking/Baselining via Shodan & Censys.io tools.

How to Find IoT Devices Connected to Your Campus Network

Why is this important?

IoT devices on our campus networks may be vulnerable to malware and increase the risk for information security and privacy compromises. Yet, many of these devices show up on campus without the knowledge of central IT. So how can we find those devices that put us at risk? The Internet2 IoT Systems Risk Management Task Force found two tools, Censys and Shodan easy for non-security experts to use to find IoT devices.

Types of Devices/ Vulnerabilities



Image Sources: IndustryBuyer, BACnet Interest Group Europe, Alibaba, Lantronix, MegaLab.

Bashlight and Mirai malware have created botnets that carried out DDoS attacks on DYN, OVH, and an unnamed US university.

- Devices with weak or hardcoded passwords: IP cameras, light sensors, refrigerators
- Devices that connect through known high risk ports such as Telnet/port 23 using TCP/IP (no encryption): printers, cameras, device servers
- Devices that connect to components of building automation systems: SCADA and ICS components

Tools: Shodan and Censys



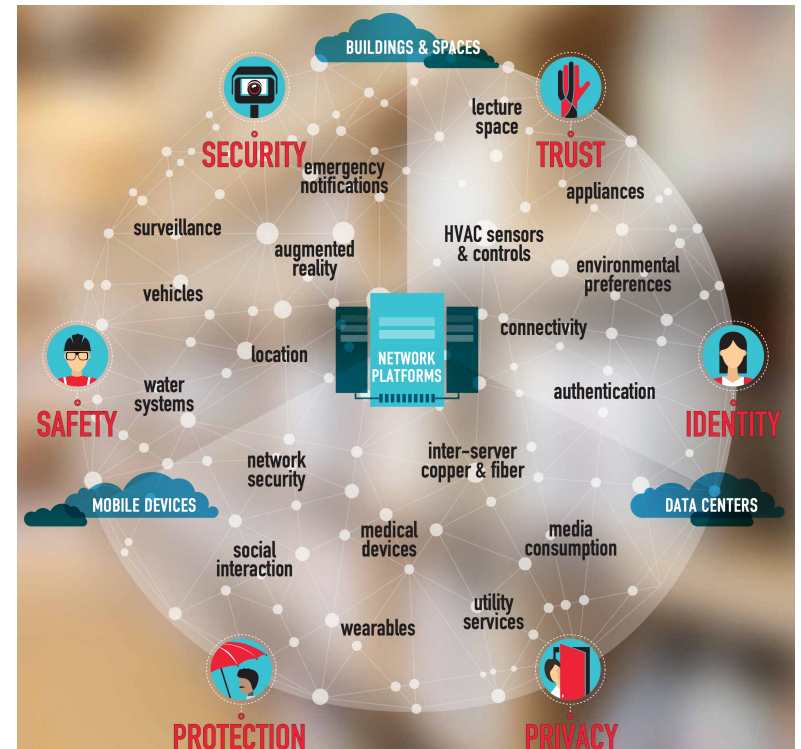
Shodan and Censys are search engines that find servers and other devices connected to the Internet that use Internet protocols specifically associated with industrial control systems and, increasingly, IoT devices & systems. They retrieve metadata about the devices such as geographic location, operating system, device name and serial number.

Join Us

Interesting in joining the Internet2 Collaborative Innovation Community and IoT Working Group? Contact the Internet2 Chief Innovation Office at CINO@Internet2.edu

Addressing TIPSS for IoT is essential to achieving safe, secure, scalable future smart city and campus architectures.

- **Trust:** Allow only designated people/services device access
- **Identity:** Validate identity of people, services, or “things”
- **Privacy:** Device, personal, sensitive data is kept private
- **Protection:** Device users protected from harm
- **Safety:** Safety of devices, infrastructure and people
- **Security:** Maintaining security of data, devices, people, etc.



Internet2 Smart Campus Initiative Next Steps

- **Increase** IoT systems risk awareness using Shodan & Censys.io, demos at Global Summit 2017 in Washington, D.C. April 23-26
- **Share** IoT Systems Vendor Requirements Document at Global Summit 2017
- **Planning Workshop** with Princeton University Center for Information Technology Policy (CITP) on TIPSS and Ethics in Campus IoT Networks, 2017
- **Create** thought leadership on TIPSS for IoT for smart & connected campus/communities
 - **Whitepaper collaborations:** Enterprise IoT Internet2-ITANA (IT Architects iN Academia) Collaboration and Internet2 Chief Innovation Office Program Advisory Group led whitepaper
- **Participate** in new community initiatives and collaborations toward a Smart Campus



Questions & Answers...

Thank You

fhudson@Internet2.edu

@FIoInternet2