Hearing on China, the United States, and Next Generation Connectivity
Testimony before the US-China Economic and Security Review Commission

Internet of Things (IoT) Systems Risk Mitigation for Universities, Cities, and Institutions
with Observations on 5G and China
March 8, 2018

Chuck Benson
University of Washington

1. Overview

Internet of Things (IoT) Systems, combined with the underlying wired and wireless infrastructure that support them, have the potential to bring substantial value to government, cities, universities, other institutions, and companies. However, without thoughtful application and awareness of process and components, IoT Systems can also bring substantial risk and exposure to those same entities.

Three broad risks of IoT Systems implementations to universities, institutions, and cities include (not in order of priority):

- Supply chain risks
- Poor selection, procurement, implementation, and management of IoT Systems
- Lack of institutional governance and lack of awareness of social-technical issues in IoT Systems deployments

Any of the above risks or, more likely, combination of these and others can have substantial negative impacts. Examples include, but are not limited to:

- Use of large numbers of compromised IoT devices to build ‘botnets’ for Distributed Denial of Service (DDoS) attacks.
    - One example is the October 2016 DDOS attacks, using Mirai malware, that brought substantial impact to Internet services such as CNN, Netflix, the Wall Street Journal, Twitter, and many others. [i] The previous month, a large scale IoT-based DDoS attack was launched against popular and prolific security researcher Brian Krebs [ii]
    - Another IoT-based botnet dubbed “Reaper” has been discovered by security researchers that appears to be substantially larger than the Mirai-based botnet used in the attacks of fall 2016. It is not known what it’s intended target may be. See Wired article, “The Reaper IoT Botnet Has Already Infected A Million Networks.” [iii]

- Use of IoT devices to facilitate attack on internal systems, to include critical infrastructure.
  - One example is the Turkish pipeline explosion of 2008 where, “by hacking the video and sensors that closely monitored the … pipeline, the attackers were able to prevent operators from learning of the blast until 40 minutes after it happened, from a security worker who saw the flames.”[iv]

- Use of IoT devices to collect and reroute sensitive information
  - On the personal level, this manifests itself in privacy issues
  - On the corporate level, this can manifest itself in corporate espionage
  - On the government/military level, this can manifest itself in intelligence collection and critical systems disruption

- Compromising life-safety medical devices. Ever increasing numbers of these devices will be deployed in individuals and across populations. Inability to manage cyber risks in this space will stifle innovation and increase liability to providers.
  - Some examples include insulin pumps, defibrillators, blood-storing refrigerators
  - Other examples include hacking medical equipment such as MRI machines[v][vi]

- Use of IoT devices and systems to cause large scale disruption in economic systems
  - Hospitals, manufacturers, others to fail
  - Long term product quality control problems
  - Short term to long term service disruption

This testimony will also propose four activities that US government can support/enhance that will help to mitigate these risks. These include:

- Standardized provenance vetting and reporting for IoT device components
- Support for increased US labor force training in Operational Technology (OT) skill sets
- Support for development of institutional and city IoT governance frameworks
- Support for data ethnography and socio-technical research and application in context of IoT Systems

These are not all of the risks that IoT Systems pose and these are not all of the potential mitigation approaches, but these constitute a good place to start.

Potential benefits of IoT Systems for universities, institutions, and cities

Potential benefits of appropriately selected, procured, implemented, and managed IoT Systems are substantial. Universities and institutions can benefit from IoT systems such as traditional building automation systems (e.g., HVAC), energy management and conservation systems, building and space access systems, environmental control systems for large research environments, academic learning systems, and safety systems for students, faculty, staff, and the public. Cities also benefit from IoT Systems supporting public safety (e.g. surveillance of high crime areas), air quality monitoring by sector, transportation control systems, city accessibility guidance and support, and many others.

The *potential* value-add of IoT Systems for institutions, cities, and government is virtually limitless. Just check the IoT page of any major or minor technology provider. For example, all of these companies [vii] have substantial presence (or at least aspirational web pages) in this space:

- Intel
- Cisco
- Microsoft
- Siemens
- Johnson Controls
- Honeywell (e.g. Tridium Niagara)
- AT&T
- Verizon
- Many others

More on potential risks of IoT Systems for universities, institutions, and cities

The *actual* value-add is less than limitless and needs to consider substantial and often non-obvious costs and risks incurred. As mentioned above, these risks include supply chain risks of components and subcomponents, failure or inability to in systems selection, procurement, implementation and management, and issues around governance and socio-technical relationships.

- Supply chain risks – what is in those thousands, hundreds of thousands or more, devices that we are deploying in our institutions and cities?
- How IoT Systems are selected, procured, implemented, and managed matters (and we're not very good at it)
- Governance and ownership of systems within a city, university, or corporation. What is the criteria for system selection? What is the criteria for performance management of the system? Is it doing what we thought it would? Do we know what we thought it would do? Is it costing what we thought it would cost?

2. Characteristics of IoT Systems, IoT Devices, and the IoT Ecosystem

a. IoT Systems are different from traditional enterprise IT systems

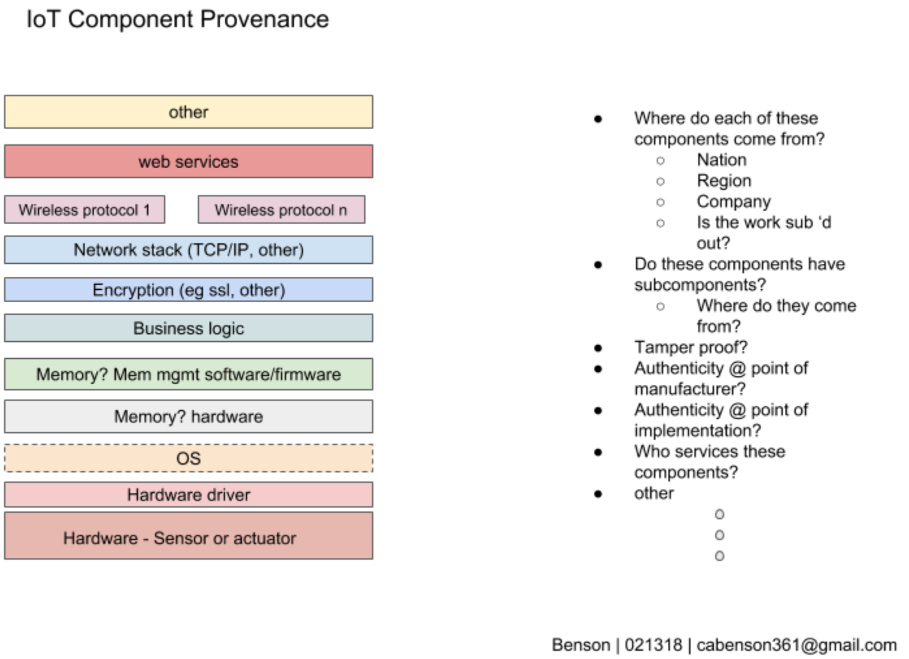
IoT systems are different from traditional IT and information management systems and require new approaches to achieve investment value as well as to maintain or enhance an institution's risk profile. Six factors distinguish IoT systems from other technology systems: (1) the large number of devices; (2) the high variability of types of devices and components within those devices; (3) the lack of language and conceptual frameworks to discuss and easily categorize and classify devices; (4) the fact that they span many organizations within an institution; and (5) the fact that the hundreds or thousands of devices embedded in the physical infrastructure around us tend to be out of sight and out of mind; (6) lack of precedence for IoT systems implementation and management.

Large numbers

In 2011, Cisco predicted that 50 billion devices will be connected to the Internet by 2020, and the growth appears to be compounding. It can be difficult to wrap one's head around the magnitude of this growth. To help, we can borrow from the "Rule of 72" used in finance, real estate, and other industries for quick and dirty approximations where the growth rate is divided into the number 72 to get an approximation of the time it takes the count of devices to double. For example, if you buy a house that increases in value at 6% per year, the time it takes to double in value is approximately 72/6 = 12 years. To use an example in the IoT space, an International Data Corporation (IDC) report suggests an 18.6% annual growth rate in the IoT market in manufacturing operations, starting with a $42 billion market in 2013.[viii] Applying the Rule of 72: 72/18.6 = 3.9, meaning the market size would grow from $42 billion to $84 billion by 2017 (an estimated 4 years).

High variability

The variety of types of devices and of the hardware and software components within each device is very high. IoT devices do numerous different tasks, including measuring building energy, video monitoring a space, reading a heart rate, and sensing air quality every few seconds in a research facility. Devices can have many different types of hardware from many different manufacturers as well as many different layers of software, each possibly from a different software company (or person). This huge variability contributes to the challenge of identifying device categories that can be helpful in developing risk management approaches. This variance also makes provenance tracking/management very difficult.



IoT Component Provenance

other

web services

Wireless protocol 1 | Wireless protocol n

Network stack (TCP/IP, other)

Encryption (eg ssl, other)

Business logic

Memory? Mem mgmt software/firmware

Memory? hardware

OS

Hardware driver

Hardware - Sensor or actuator

- Where do each of these components come from?
  - Nation
  - Region
  - Company
  - Is the work sub ‘d out?
- Do these components have subcomponents?
  - Where do they come from?
- Tamper proof?
- Authenticity @ point of manufacturer?
- Authenticity @ point of implementation?
- Who services these components?
- other

Benson | 021318 | cabenson361@gmail.com

In their paper, “Internet of Things Device Security and Supply Chain Management,” [ix] researchers Lee and Beyer contribute:

> “… policies relating to electronic supply chain security at national level are lacking … although companies try their best to follow piecemeal governmental and industry guidelines for supply chain security, this vigilance is only as strong as a company’s dedication to security.” [Supply chain policy shortcomings] “… arise because cybersecurity issues are highly complex and difficult for policymakers and industry leaders to reach agreement upon.”

Lack of language

We do not have commonly accepted language or conceptual frameworks for talking about the IoT and these systems. Without a shared language, planning IoT systems implementations or managing risk around systems is very difficult. It is also challenging to establish standards and vendor contract performance expectations without this language.

Spanning many organizations

IoT systems tend to span multiple organizations within a higher education institution. For example, environmental control systems for large research spaces are rapidly increasing in number. These systems often sense and regulate air temperature, humidity, particulate levels, light, motion, and many other factors. These measurements are used for safety, energy efficiency, regulatory compliance, and other research needs. Implementing an environmental control system will likely involve an institution's central IT organization, the facilities management group, the researcher/principal investigator, distributed/local IT organizations, and at least one and probably several vendors. Between these organizations are gaps through which systems accountability and ownership can fall. For example, the researcher thinks that the central IT organization is monitoring and managing the system and keeping it secure. At the same time, the central IT organization doesn't know what is being plugged into the network backbone. Each one hopes the other is managing the system well. Because of this spanning nature of IoT systems, there is often no overarching visibility, much less ownership and accountability, for the whole system.

Out of sight, out of mind

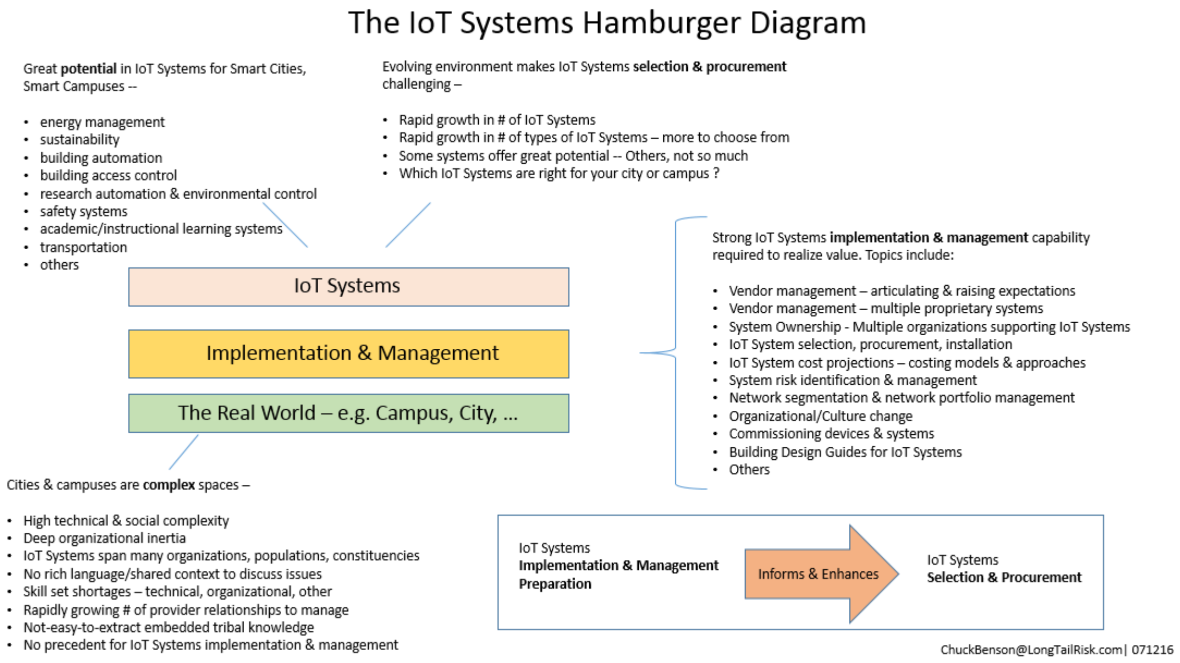
Finally, IoT systems are unique in that many of the technical parts of the IoT system—that is, the computing and networking endpoints—are built into the physical infrastructure, out of sight and out of mind. A smart grid or campus energy management system can easily have thousands of networked, computing, sensing endpoints that are built into campus buildings. We don't think about them because we don't see them.

Lack of precedence for implementation

Institutions, cities, and companies have very limited precedence for IoT Systems selection, procurement, implementation, and management. There is not a depth of history of implementations, colleagues with depth of experience to ask, or even competitors with depth of experience to observe. These technology (IoT) systems are now being thrown into traditional capital development, construction, and facilities operations organizations and implementing complex technology systems is not a part of the history or experience of these disciplines. Similarly, with an IoT System's broad geographical distribution of devices, requirement for trades skill to access these devices, and other factors, implementing IoT Systems is unfamiliar territory for central IT organizations as well.

b. How IoT Systems are implemented is critical

How IoT Systems are implemented is critical to successful implementation. Universities, cities, and other institutions have a substrate of historical complexities, organizational structures, skill set issues, and other factors. Selecting, procuring, implementing, and managing an IoT System to such a substrate is a critical endeavor and one in which we have little experience.



The IoT Systems Hamburger Diagram

Great **potential** in IoT Systems for Smart Cities, Smart Campuses --

- energy management
- sustainability
- building automation
- building access control
- research automation & environmental control
- safety systems
- academic/instructional learning systems
- transportation
- others

Evolving environment makes IoT Systems **selection & procurement** challenging –

- Rapid growth in # of IoT Systems
- Rapid growth in # of types of IoT Systems – more to choose from
- Some systems offer great potential -- Others, not so much
- Which IoT Systems are right for your city or campus ?

IoT Systems
Implementation & Management
The Real World – e.g. Campus, City, …

Strong IoT Systems **implementation & management** capability required to realize value. Topics include:

- Vendor management – articulating & raising expectations
- Vendor management – multiple proprietary systems
- System Ownership - Multiple organizations supporting IoT Systems
- IoT System selection, procurement, installation
- IoT System cost projections – costing models & approaches
- System risk identification & management
- Network segmentation & network portfolio management
- Organizational/Culture change
- Commissioning devices & systems
- Building Design Guides for IoT Systems
- Others

Cities & campuses are **complex** spaces –

- High technical & social complexity
- Deep organizational inertia
- IoT Systems span many organizations, populations, constituencies
- No rich language/shared context to discuss issues
- Skill set shortages – technical, organizational, other
- Rapidly growing # of provider relationships to manage
- Not-easy-to-extract embedded tribal knowledge
- No precedent for IoT Systems implementation & management

IoT Systems
Implementation & Management Preparation
Informs & Enhances
IoT Systems
Selection & Procurement

ChuckBenson@LongTailRisk.com| 071216

c. Measuring success of an IoT Systems Implementation for a university or city

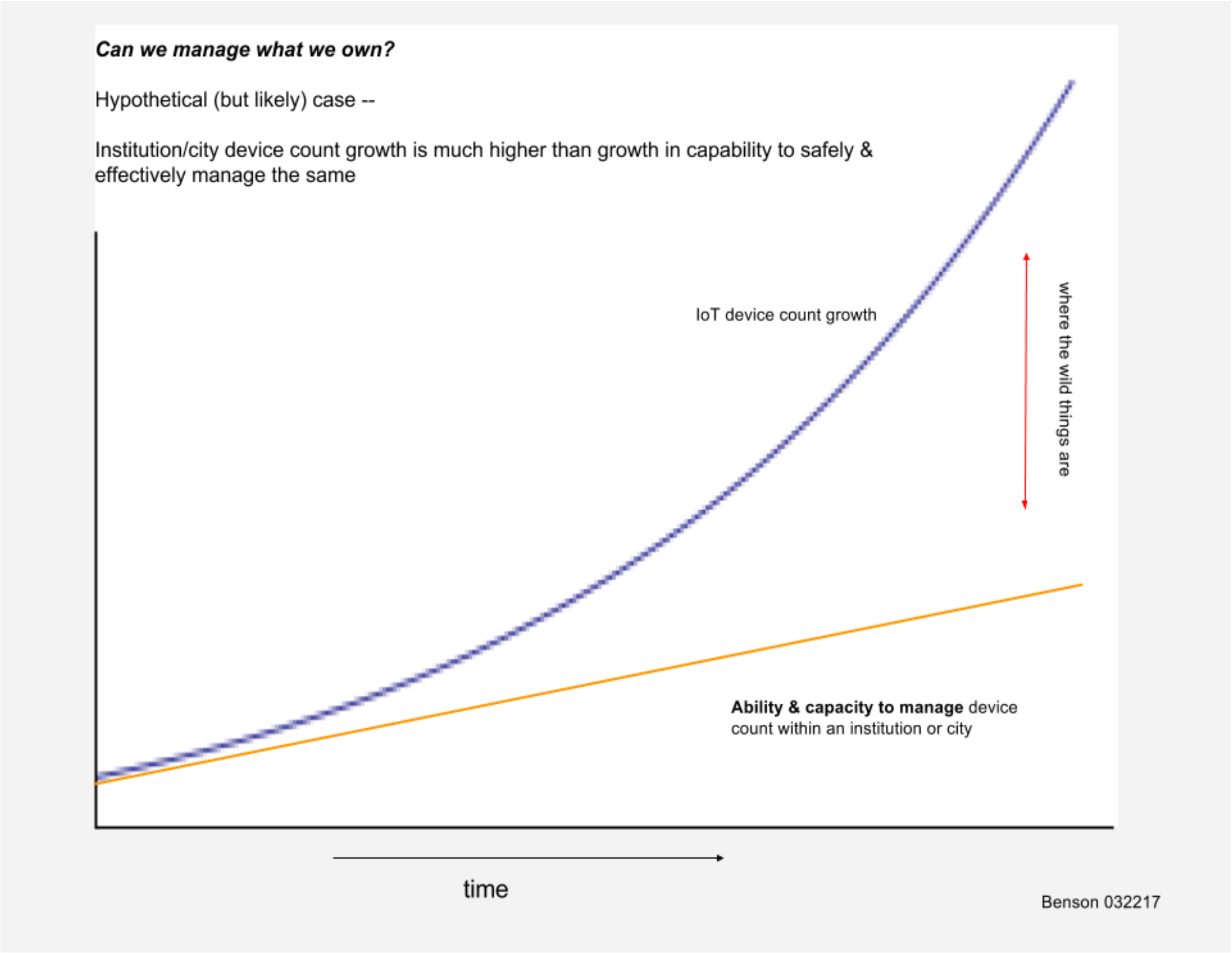
Two overarching factors that can help measure or determine success for an IoT Systems implementation in a university or city are:

- ROI
  - Does the IoT System do what was expected and *deliver the value that was expected* at the *actual costs incurred* (vs projected costs)?
- Cyber risk
  - Did *implementation* of the IoT System make the cyber risk profile for the university or city worse?

Regarding the first — ROI, does the system do what we thought it would do at the costs/investment that we thought would be incurred? Determining costs of IoT Systems implementation is different from traditional enterprise systems. Most institutions and cities have little experience at it and are generally not very good at it. Further, other subtleties such as expectations of the data [x] created from deployed IoT systems across a spectrum of populations, demographics, and constituencies directly impact perceptions of system (and investment) success.

Regarding the second — cyber risk profile, did the IoT System implementation make things worse for the institution or city? Cyber risk profile degradation for an institution can come from poorly configured devices, insufficient management resources (skill, capacity) to support IoT devices and data aggregators/controllers, inadequate vendor management, and others.

d. IoT Systems Manageability



A key component to both IoT Systems ROI and changes to cyber risk profile is the *manageability* of the IoT System.

> *IoT Systems — with their* multi-organizational boundary spanning [xi]*, unclear systems ownership and accountability, lack of precedence for implementation, and high number of networked computing devices ('Things') — are particular candidates for unmanaged/under-managed systems in a city or institution.*

IT systems that tend to be more manageable allow for more predictability in an institution's resource and cash flow planning. Criteria for high systems manageability include:

- having well-defined performance expectations
- thoughtful, thorough, and integrated implementation
- accessible training and documentation
- strong vendor support and strong vendor relationships
- others

Unmanaged or under-managed systems increase the likelihood of a cyber event such as device compromise or whole system compromise as well as facilitate potentially substantial operations disruption and unplanned financial burden.

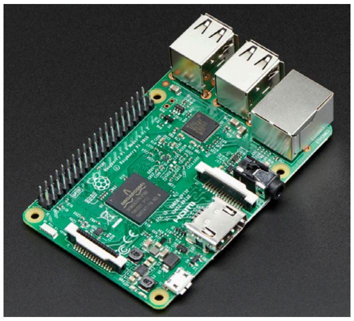
e. Low barriers to entry -- Makerspace, Raspberry Pi's, Arduino's, Adafruit, and …

It is increasingly easy to create the 'Thing' in the Internet of Things. The 'T' in IoT is a device that:

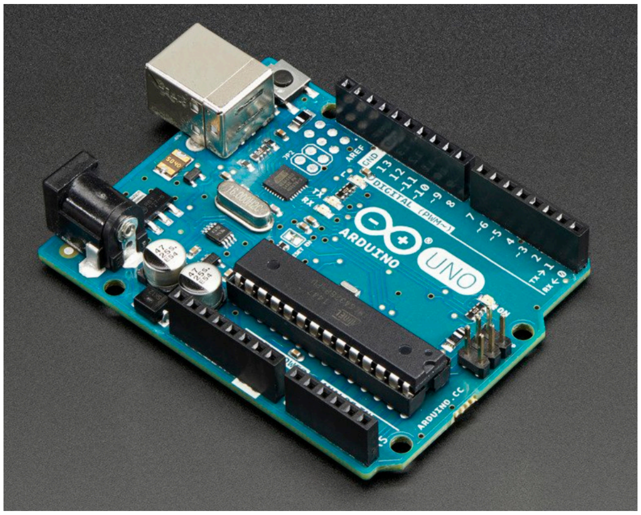
- is networked
- computes
- interacts (senses or changes) the local environment in some way

Whether hobbyists, participants in the Maker/Makerspace [xii] movement, commercial developers, or some combination, there are more and more components – simple and sophisticated, accessible development platforms, training, vendor support, and community-based support that facilitate IoT device and systems development. Three examples:

- Raspberry Pi [xiii]. The Raspberry Pi, developed and released in 2012 out of the UK, is a full featured computer the size of a deck of cards originally designed for education that costs approximately $35. It supports multiple Linux-based operating systems and has a very rich set of features to include wireless support, video (HDMI) support, audio support, input/output for attaching sensors, actuators, and other devices. Importantly, it has strong and broad community support.



- Arduino [xiv] . The Arduino, developed and released in 2003 out of Italy, is also a full-featured computer at a cost of ~$30. Though the Arduino operates without the support of a traditional operating system such as Linux, it has strong development tools, and a huge community support base. It can be argued that this small computer kicked off the Maker/Makerspace revolution.



- Adafruit [xv] was founded in 2005 by MIT engineer, Limor "ladyada" Fried. Adafruit sells electronics components such as Arduino and Raspberry PI. The company also designs, makes, and sells its own products as well in additional to a wide array of support tools and components. Importantly, the company has an increasingly sophisticated training program for device design and production. The founder was also featured on the cover of Wired magazine in March 2011.

f. Cloud services in direct support of IoT System and device deployment

There are rapidly evolving cloud platforms to support IoT device/system development and deployment. IoT devices and systems often go hand in hand with cloud-based services. These are also easy to access and are becoming less and less expensive. These cloud services are designed specifically for IoT devices and systems and there is substantial competition between them to garner IoT space mind and market share. Examples of IoT cloud services include:

- AWS IoT [xvi] -- with web tag line – “A system of ubiquitous devices connecting the physical world to the cloud.”
- Google Cloud IoT [xvii] – with web tag line – “Platform for intelligent IoT services”
- Microsoft Azure IoT Suite [xviii] – with web tag line – “Capture and analyze untapped data to improve business results”

These are just a small subset of the cloud services being offered to support IoT devices and IoT systems. Many cloud service solutions will, in fact, incorporate one or more other cloud services.

g. Shodan & Censys: Freely available attack research tools/risk mitigation tools

There's good news and bad news when it comes to getting a quick snapshot of an institution's public-facing IoT systems exposure. The good news is that tools for doing this are publicly available. The bad news is that tools for doing this are publicly available. Anyone—those in institutions and cities as well as those criminal and nation-state actors with malicious intent—can use the same tools. However, since those with malicious intent are most likely using their own, nonpublic approaches, these publicly available tools might well be a net benefit to higher education (if we use them).

Shodan [xix] a private endeavor, is the best-known of these public tools and has been around the longest. Censys [xx], stemming from research at the University of Michigan and the University of Illinois at Urbana-Champaign, is the newer entry into the space. Although their approaches are different, the two tools do similar things: they scan (almost) all publicly available IP addresses, record the responses, and make the IP addresses, responses, and metadata (e.g., location and timestamp data) available to the public. The scans look for devices often associated with IoT and traditional industrial control systems. Both tools have the ability to download data, and they offer APIs that allow direct access for further analysis. So, by using either or both tools and searching the IP address space of a campus, institutional IT leaders can get an idea of current exposure—results that can be surprising.

h. Socio-technical and cultural aspects of successful IoT Systems integration

There are substantial socio-technical aspects to implementation of IoT systems on university campuses, cities, and others. With widespread IoT device sensing, data creation, data aggregation, analytics, and business and social decisions made on the same, we are in a new world. Three aspects of this new world include:

- How IT and built environments technology worlds come together
- How constituents of an IoT System perceive value of the system
- Governance

Blending Information Technology and Operational Technology

To the first point, the technology deployed in built environments (buildings, campuses, cities, etc.) is often called Operational Technology (OT). This is the technology device that senses the environment (e.g. outside air temperature, electrical power consumption, measures heat usage in a building, or other) and/or interacts with the environment (e.g. makes a remote HVAC thermostat or blower setting change, moves a networked video surveillance camera, or other).

These professional skill sets that deploy, configure, manage, and monitor these sensors and actuators *are in short supply*. These skillsets are a cross between traditional trades skill sets (such as electricians) and IT skill sets (with software configuration and testing skills). The skill sets are in short supply and in high demand. Without them, deployment demand for IoT Systems (or 5G) cannot be met and the risk of systemic (e.g. thousands or more of devices) misconfiguration and lack of ongoing IoT systems support is very high. This misconfiguration/poor configuration, in turn, results in lost ROI and a substantially degraded security posture for the campus, city, or institution.

Adding to the challenge is that the skill sets of traditional IT and traditional OT have very different cultural backgrounds. Historically, the professional deploying the OT device has come from a building and maintenance background, for example a facilities management or construction organization. Because these professionals build and/or maintain buildings expected to last decades, they tend to think in terms of decades – long term support of an operational building. Further, these professionals, understandably, tend to be motivated not to change a system (electrical power delivery, heat delivery, as examples) that is working -- something of an, "if it ain't broke, don't fix it" approach. IT professionals, on the other hand tend to think in terms of months, weeks, and days and they are frequently changing software configurations, software versions, etc. in an attempt to keep up with newly discovered vulnerabilities and types of attack that are discovered almost daily.

The differences in the cultural mindsets of these two professions become readily apparent as IT and OT professionals and teams come together to implement and manage IoT systems. Successful, risk-mitigated systems implementation requires mature, experience skill sets that can navigate the blending of these two historically disparate cultures. And again, these skill sets are in short supply.

Understanding data expectations is essential to IoT Systems & smart city success

One of the subtle but powerful factors affecting IoT Systems implementation and management success in complex organizations such as a smart campus or smart city is *the organizational and cultural change required in becoming a data-centric organization.*

In most cases, this is not a small transition. The evolutions of these cities and institutions has been from a place of relatively limited data available across multiple contexts. When an organization begins to shift, or seeks to shift, to an organization where data production, acquisition, consumption/analysis, and management – such as that coming from an IoT System -- are core to its operation and to its perception of self, subtle but powerful cultural and organizational change is required.

Data generation and/or acquisition is a major component in almost all IoT Systems that may be deployed in support of smart campuses and smart cities. *Data creation and data actionability is often where much of the value is derived from an IoT System deployment.* The challenge is that the expectations of data from the many constituencies and consumers can vary in significant ways and these variances in expectation, in turn, influence perceptions of IoT Systems, and in turn smart city system, success. Further, *early IoT System implementations that are viewed as failures not only mean lost investment on those particular systems, but also that these failures will (understandably) make constituents wary of funding or deploying subsequent systems.*

Reflecting on and planning for what expectations of data are in different constituencies and contexts can substantially help identify criteria for perceptions of successful IoT Systems implementations and smart city deployments.

Institutional governance – one example – our approach at the University of Washington

Governance and guidance for IoT Systems implementations in most universities and cities is nascent. At the University of Washington, we have instantiated and operated task forces to profile the problem of growing IoT Systems risk as well as plan for mitigation of the same. For example, we ran the Protection of Industrial Control Systems task force in 2013-2014 and the University of Washington (UW) Compliance IoT Systems Risk Mitigation Task Force (current). This latter task force has reports to University of Washington Regents which reflects the university's growing awareness and intention of the effort. The university also supported my effort of chairing a national IoT Systems Risk Management Task Force for Internet2 [xxi].

Our current effort, the University of Washington Compliance IoT Systems Risk Mitigation Task Force, seeks to:

- Increase awareness of IoT Systems risks and benefits in all facets of the institution
- Provide guidance and oversight for IoT systems selection, procurement, implementation, and management
- Increase inter-organizational coordination for managing IoT Systems across the institution
- Identify clear IoT Systems owners within the university
- Establish robust expectations for IoT Systems vendors and providers
- Identify a workable IoT System and device classification and categorization to assist in managing risk
- Propose an institutional governance structure for providing oversight to IoT Systems deployments

Participating organizations and roles within the university include:

- Major and minor capital development
- Planning and budgeting
- Energy management and conservation
- Central IT
- Facilities management
- Academic research
- UW Office of Chief Information Security Officer (CISO)
- UW Medicine Office of Chief Information Security Officer (CISO)
- Institutional privacy official office
- Enterprise risk management and compliance office

While there is more work to be done, Task Force-led directed discussions and related efforts involving these multiple organizations and departments are already creating benefit in terms of increased awareness and enhanced communication on the topic IoT Systems implementation and risk mitigation.

3. Observations on IoT, 5G, and China

IoT and 5G

I am not an expert on 5G, but I can make observations based on existing IoT deployments with existing wired and wireless approaches and my understanding of potential 5G features and capabilities.

Fully deployed and managed, 5G purports [xxii]to deliver benefits that include:

- Increased bandwidth
- Support of increased device count

- Reduced latency

The effects of a fully-deployed, as advertised 5G system would serve as an effect multiplier for IoT Systems in universities, institutions, and cities. That is, there would be:

- More potential value-add and potential social benefit because of increased capacity and feature sets of part of the network supporting IoT devices and systems
- More cyber risk and potential for lost investment if systems are not thoughtfully implemented

Another aspect that would also act as a multiplier would be that a deep and broad and fully-deployed 5G network could allow IoT Systems providers to ‘hop over’ constraints of existing city, university, and other institutional legacy network systems.

Importantly, there is still capacity for IoT Systems evolution with existing wired and wireless technologies. A fully-deployed, functional, and well-managed 5G system would add more capacity for IoT Systems development, but there is still room to work with existing wired and wireless deployments.

Also important to note is that a full-featured, deep, and broad 5G deployment will require:

- Increased technical (OT) support for the more numerous and dense small cells and antennae required of 5G technology
- More negotiation and bureaucratic/relationship navigation between vendors, cities and institutions for issues such as utility pole use and other spaces for cell/antenna deployment

From my point of view, it is not clear that these issues can be addressed quickly or easily.

Because of these uncertainties, a systematic approach to 5G deployment in the United States is highly desirable. A rushed approach would only exacerbate the non-trivial risks stemming from IoT Systems implementation.

Two comments on IoT and China

An anecdote on electronic component provenance

While the following anecdote is certainly not indicative of all manufacturing processes, it has always stuck in my mind as a reminder that not everything, i.e. electronic component, may be where I think it’s from or coded the way I think it’s coded.

Andrew (‘bunnie’) Huang, MIT electrical engineering PhD, and his business partner Sean (‘xobs’) Cross [xxiii] gave a talk at the 2013 Chaos Computer Congress [xxiv] on hacking SD cards. SD cards are the removable memory cards that go into digital cameras and other electronics.

In the course of the presentation, Huang describes vast bins of memory cards of ranging quality, size, and performance in the market of Huanqiangbei in Shenzhen, China. He talks about card relabeling as a common practice to adjust for sub-performing cards as well as card factories that have very few access controls regarding what configuration files are written to cards and chips and how they are configured. Transcribing from the presentation video (at approximately 50:45):

> “.. when we’ve been to the factories where they burn [program] the firmware in, you can basically just walk in and go up to the burner [component programmer] and replace the files on it … literally, there were chickens running through the factory … there’s no security, there’s no badges … they make these things [components] and ship them all over the world …”

My previous naïve assumption that all electronic parts were created and programmed in carefully controlled and audited environments was appropriately debunked. Many buy from this kind of loosely controlled electronics market because the components are very inexpensive compared to a highly regulated manufacturer. IoT devices have many of these kinds of components.

A view of the Maker culture in China

IoT devices are a core component of many “Maker” activities. The February/March 2018 issue of the popular Make magazine has a section focusing on the Maker culture in China. The Maker culture, in turn, is substantially supported by and enhanced with IoT technology. [xxv]

One author, a 23 year old woman from Shenzhen, speaks of establishing the first Open Source Hardware Association certified project in China. She states that Shenzhen used to be known as the cloned/copycat capital of the world but that that is no longer the case. She also has a YouTube channel [xxvi] dedicated to her Maker work.

Another writer in the issue is the Director of the International Collaboration of the Shenzhen Open Innovation Lab. She discusses helping to organize the "Maker Workshop in the National Mass Innovation and Entrepreneurship Week – a major national event to promote innovation policy by the Premier Li Keqiang." She also discusses Maker partnerships with other countries to include Britain, Nigeria, Ethiopia, Peru, and Pakistan.

A third contributor is the general secretary of the Shenzhen Industrial Design Association (SIDA) which works to "promote the importance of industrial design to government and business." SIDA has over 700 institutional members and works with "over 100,000 industrial designers in Shenzhen." Further, she says,

> "Today, Shenzhen has one of the best government policies in the world to encourage creativity and innovation in industrial design … and the Shenzhen Industrial Design Faire has become the largest industrial design event in the world."
>
> "…Shenzhen industrial designers … help Shenzhen manufacturers move up the value chain … and building the bridge between global makers and the Shenzhen ecosystem …"

These attestations by the article's authors convey a very active, substantial, and growing IoT and Maker effort at the individual and group level that is being integrated with robust industrial design approaches. This integration and mutual leveraging of efforts will only continue to drive the IoT movement in China.

There is also an increasing amount of IoT curricula in United States schools and programs. [xxvii] It is not clear to me whether China or the US as the advantage in this pipeline.

4. Recommendations

While there are many opportunities for the US Government to help, both in terms of IoT Systems risk mitigation and enhanced value from IoT Systems, four recommendations are below.

1. Develop a standard system for reporting electronic component provenance of firms developing IoT devices and systems
    a. NIST, ISO, SAE and others have done some work here [xxviii]
    b. It is important that this system is implementable in practice
        i. Balance is needed between thoroughness and pragmatism
        ii. Approaches that are overly burdensome will not be adhered to and thus be ineffective
        iii. Burden will vary with firm size

2. Fund and support development of operational technology (OT) skill sets
    a. The current shortage of these critical skill sets contributes to:
        i. poorly implemented systems,
        ii. increased cybersecurity risk to institutions and cities,
        iii. reduced opportunity for value-add and returned investment

3. Fund and support development of governance frameworks for cities and institutions
    a. Universities, cities, and institutions can use these frameworks as templates for their own organizations that they can continue to evolve to meet their needs

4. Fund and support data ethnography and social-technical science research as it relates to IoT Systems.
    a. Interpreting and mediating the unprecedented amounts and types of IoT Systems data is a very new space for universities, institutions, and cities and is critically important.
    b. Data ethnography and other social-technical research can be used to inform institutional and city leadership as they become increasingly immersed in, affected by, and dependent up IoT systems.

References:

[i] "2016 Dyn cyberattack", Wikipedia, https://en.wikipedia.org/wiki/2016_Dyn_cyberattack, accessed March 4 2018

[ii] Brian Krebs, "Krebs on Security Hit With Record DDOS", https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/, September 21 2016

[iii] Andy Greenberg, "The Reaper IoT Botnet Has Already Infected A Million Networks", https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/, October 20, 2017

[iv] Dan Goodin, "Hack said to cause fiery pipeline blast could rewrite history of cyberwar", https://arstechnica.com/information-technology/2014/12/hack-said-to-cause-fiery-pipeline-blast-could-rewrite-history-of-cyberwar/, December 10 2014

[v] Rachel Arndt, "Hacked medical devices could wreak havoc on health systems", http://www.modernhealthcare.com/article/20180120/NEWS/180129999, January 20 2018

[vi] Kim Zetter, "It's insanely easy to hack hospital equipment", https://www.wired.com/2014/04/hospital-equipment-vulnerable/, April 25 2014

[vii]Intel -- https://www.intel.com/content/www/us/en/internet-of-things/overview.html
Cisco – https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html
Microsoft – https://www.microsoft.com/en-us/internet-of-things
Siemens -- https://www.siemens.com/global/en/home/products/software/mindsphere.html
Johnson Controls -- http://www.johnsoncontrols.com/buildings/specialty-pages/iot
AT&T -- https://iotplatform.att.com/
Verizon -- http://www.verizonenterprise.com/products/internet-of-things/

[viii] "New IDC Forecast Asserts Worldwide Internet of Things Market to Grow 19% in 2015, Led by Digital Signage," press release, May 19, 2015.

[ix] Stacia Lee, Jessica Beyer, "Internet of Things Device Security and Supply Chain Management," https://www.wilsoncenter.org/publication/internet-things-device-security-and-supply-chain-management , November 22 2017

[x] Chuck Benson, "Understanding data expectations is essential to IoT Systems and Smart City/Smart Campus success", http://longtailrisk.com/2016/07/27/understanding-data-expectations-key-iot-systems-smart-city-success/, July 27 2016

[xi] Chuck Benson, "Organizational-spanning characteristics of IoT systems", http://longtailrisk.com/2016/06/07/organizational-spanning-characteristics-iot-systems/, June 7 2016

[xii] "Maker culture", Wikipedia, https://en.wikipedia.org/wiki/Maker_culture, accessed March 2 2018

[xiii] Raspberry Pi, https://www.raspberrypi.org/, accessed March 2 2018

[xiv] Arduino, https://www.arduino.cc/, accessed March 2 2018

[xv] Adafruit, https://www.adafruit.com/about, accessed March 2 2018

[xvi] AWS IoT, https://aws.amazon.com/iot/, accessed March 2 2018

[xvii] Google Cloud Platform, https://cloud.google.com/solutions/iot/, accessed March 2 2018

[xviii] Microsoft Azure IoT Suite, https://azure.microsoft.com/en-us/suites/iot-suite/, accessed March 2 2018

[xix] Shodan, https://www.shodan.io/, accessed March 2, 2018

[xx] Censys, https://censys.io/, accessed March 2 2018

[xxi] Internet2, https://www.internet2.edu/about-us/, accessed March 4 2018

[xxii] Sascha Segan, "What is 5G?", PC Magazine, https://www.pcmag.com/article/345387/what-is-5g, accessed March 3 2018

[xxiii] Ebony Calloway, "Engineer Spotlight: bunnie and xobs and the Essential Guide to Electronics in Shenzhen", July 27 2016

[xxiv] Andrew 'bunnie' Huang, Sean 'xobs' Cross, "The Exploration and Exploitation of an SD Memory Card," 2013 Chaos Computer Congress, http://www.bunniestudios.com/blog/?p=3554, comments at time 50:45

[xxv] Naomi Wu, Vicky Xie, "Shenzhen Standouts", Make magazine, February/March 2018

[xxvi] Naomi Wu, YouTube Channel, https://www.youtube.com/channel/UCh_ugKacslKhsGGdXP0cRRA, accessed March 2 2018

[xxvii] Jeffrey Voas, Phillip Laplante, "Curriculum Considerations for the Internet of Things", https://www.computer.org/csdl/mags/co/2017/01/mco2017010072.html, January 2017

[xxviii] NISTIR 8200, "Interagency Support on Status of International Cybersecurity Standardization, https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf