www.pipelinepub.com
Volume 16, Issue 10

From Smart Cities To Smart Nations

By: Mark Cummings, Ph.D., Bill Yeack

As it has evolved, the Internet of Things (IoT) has spawned a sister concept: the Smart City. In a Smart City, all of the city's infrastructure is instrumented, automated, and interconnected with its citizens. In many parts of the world, Smart City has just been a discussion topic, but in a few places, there have been some early implementations. Some individual cities are deploying their own incompatible solutions. As the space matures, there will be a move to Smart Nations.

In today's early stages of this maturation process, innovation is critical. This means different cities trying different non-compatible approaches. As maturation and innovation unfolds, telcos must determine whether this opportunity represents a new, profitable revenue source or whether it will be captured by superscalers such as AWS, Google, and the emerging specialized IoT Communication Service Providers.

In this competition, the telcos have four critical advantages. They are perceived as more trustworthy in maintaining privacy. They are recognized as having the highest reliability. They also have important existing relationships with key customers in the space. Finally, telcos have demonstrated experience in deploying, maintaining and operating extremely large networks of geographically dispersed resources. Security and privacy will be key issues. To successfully capture this opportunity, the telcos need to add orchestration overlay technology. Such technology will meet the requirements for cost performance, security and privacy, as well as link the cities while they try different things. Building this technology requires a software innovation vendor ecosystem. This requires change, and

change is never easy. If telcos are to remain viable, however, in a rapidly changing world, they need to find ways to change as fast as their customers are changing.

The Opportunity

Historically isolated local governments have begun talking about and working on Smart Cities. Las Vegas is an example of a city discussing a possible Smart City prototyping project. Toronto started one, then stopped. Singapore has been an early deployer of Smart City projects. Because Singapore is both a city and a state, it has avoided the question of inter-city interoperability. While the Australians have put aside their regional differences to drive national Smart City adoption, individual cities may have developed individual advantages. It is clear, however, that the major Australian cities are working to harmonize their advances.

Stages of Maturity

Today's evolution to Smart Nations is similar to how the web evolved—in spurts and stops. To understand this process, it is helpful to have a reference model of the stages of this evolution. The following section explains levels of maturity from two perspectives: individual access to information and system-wide improvements to infrastructure. There are many additional perspectives. A broader range of these perspectives will be discussed in a follow-on article.

Generation 0

Generation 0 entails the simple sharing of information from various city infrastructures with added security. Residents have secure access to information in an electronic form while preserving privacy. As an example, they could look up water usage data online.

Generation 1

In Generation 1, secure bi-directional actionable data is available, as well as orchestration that links information sources. The goal is to provide actionable data that can be used to influence outcomes with a very secure layer. As an example, residents can have online interaction to help lower their electricity costs.

Generation 2

This maturity stage involves orchestration to deploy large scale of sensors and actuators and "Whole of City" consolidation. The goal is a consolidated citizen view of all services provided, as well as a real-time view with detailed granularity of

infrastructure. For example, citizens would have one view of the services they consume in one easy-to-use place. They would be able to see adaptive traffic signals base on types and direction of traffic highs and lows, events, and emergencies.

Generation 3

This stage represents the evolution to user-based interaction from service-based interaction—from tasks to goal-based actions. There is automated orchestration for optimization and security. Seamless interaction is available from a personalized portal that integrates public and private entities to provide citizens with a single view of their data and interaction with the community. City infrastructures are highly secure and efficient. For instance, a citizen could subscribe to a street parking scheme that allows them to pay the meter over the phone. With new technology, they would be directed to the street parking space the app has reserved. Payment is automatic. In another scenario, early and effective monitoring of epidemics is available based on traffic flow.

Generation 4

The final maturity stage is marked by the emergence of Smart Nations. Orchestration and automation are happening on a national scale. National infrastructure is highly secure and efficient. Regardless of where a citizen lives, definitions and interactions are common and constant. For example, if one travels from Adelaide to Melbourne, he or she will have a single interface with the whole of local, regional and national infrastructures. This user-based action model represents the rise of citizen services rather than consumed services.

Early on there has been a lot of concern about privacy. This concern is justified. Initially, the concern focused on government surveillance. As the use of data by the superscalers has become better understood, privacy concerns have broadened. Google and Toronto started on a Smart City project only to be faced with strong resistance based on public concerns about privacy (this also represents one of the telco industry's strengths).

Although privacy concerns are at forefront now, cybersecurity will be seen as of equal or greater importance. It is a critical failure point. There are many new bad actors out there and cybersecurity is a key to preventing a major failure. Beyond just a Smart City being compromised, an entire Smart Nation could be held hostage. The view from Israel is particularly interesting in this regard: "Smart sensors and other IoT devices can dramatically boost the efficiency and effectiveness of city services—but they also increase the attack surface and risk. In fact, Gartner

predicts that CIOs and CISOs will soon be securing three times the number of endpoints compared to just a few years ago. And unlike desktops and servers, IoT devices don't support agents—making them unmanaged, unpatched, and invisible to IT teams. Ransomware and targeted attacks can lead to disruption of crucial city services and infrastructure, potentially leading to safety incidents and collapse of vital social and economic systems. As a result, Smart City deployments should always be accompanied by IoT security strategies incorporating agentless, network-layer security to provide continuous IoT asset management, risk and vulnerability management, and threat monitoring."Omer Schneider, former national intelligence officer and CEO,CyberX.

Thought leaders are recognizing the serious potential threats that come from increasing the attack surface with Smart City technology. So, it is becoming recognized that in addition to commercial security, nations' security and intelligence organizations need to extend their leadership role. Australian has been a leader in this: "In 2018 the Australian Government implemented the Security of Critical Infrastructure Act that seeks to manage the complex and evolving national security risks of sabotage, espionage and coercion posed by foreign involvement in Australia's critical infrastructure.

Australia has defined critical infrastructure as: Those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defense and ensure national security. The Act ensures that the Australian Government has access to information necessary to conduct risk assessments and the power to enforce mitigations if they are not implemented through collaboration with the critical infrastructure owners." Sean Hugo, Assistant Secretary, DCISO, Cyber Risk Services, Technology and Major Capability, Department of Home, Affairs Commonwealth of Australia.

The Smart City technology may also have effects on individual attack surfaces. Data about what individuals are doing where and when can be used by criminals. Thus, protecting the infrastructure is necessary but not sufficient. Individuals must be protected as well. Diana Neuman, Executive Director of Bace Cybersecurity Institute, notes that, "The evolution of networks followed similar patterns and security and privacy was added too late to be integrated into the framework, costing 30 years and billions of dollars trying to patch solutions for individual risks."

Capturing the Opportunity

Smart Cities are based on instrumenting the infrastructure with small, low-cost sensors and actuators. Intelligence is then applied to the data to make decisions that make things work better. Connecting this all up is a fundamental requirement. Wireless communications are considered key because of the large number of sensors and actuators involved, and the range of types of placement. Many of these sensors and actuators will not have access to the electrical grid. So, low power operation is considered a fundamental requirement. Low power requires very efficient communications. Also, because of the numbers involved, the cost of communication per node must be extremely low.

Telcos have a good foundation of experience in fielding ubiquitous wireless connectivity. However, to be successful in the Smart City space, they must dramatically lower their costs and power consumption. Some see latency as an issue, too. Experience with adding 5G core functionality to 4G networks along with other initiatives is showing some promise in these respects.

One of the key problems cities will face is deploying and configuring the large numbers of nodes. Doing this manually is intractable. Automated orchestration is the only feasible way. Here, telcos significantly trail the superscalers. Automated orchestration can also dramatically lower telco infrastructure costs. This is an area where telcos must apply themselves if they want to be able to even enter the game. Ms. Neuman's insight here is particularly significant: "Configuration management is one of the trouble spots today. As systems become more and more complex, it becomes easier and easier to make a configuration mistake or forget to set a critical option leading to higher risks of failure or compromise."

Although basic connectivity can be valuable, the really profitable area will be the provision of intelligence. In large central site systems, superscalers have a commanding lead. But the real opportunity is in distributed intelligence. This is because of both the large number of nodes and the requirement to act locally and quickly (a future article will feature an in-depth technical discussion on this subject). In this distributed area, the playing field is more level and telco experience with base station nets may give them a slight lead.

So, the path to success at the city level is a combination of orchestration and distributed intelligence. What about the move to Smart Nations? Historically, the way to make sure that Smart Cities could be integrated into Smart Nations was to impose strict standards early in the process. The problem with this is that it inhibits innovation. It prevents different cities from experimenting with different

approaches, technologies, business models, etc. In addition to crushing innovation, it makes it hard for individual cities to design systems that meet their unique situations. For example, a port city like Amsterdam might have very different requirements than Paris, France, or an agricultural hub like Kearney, Nebraska in the US.

Another approach is to have one company do all the cities. This is like the old Bell System in the US. Google (as above) has already raised its hand to do this.

In today's software-centric world, none of these old approaches is required. There are sure to be those whom, from personal interest or old habit, recommend them. But they aren't necessary. It is possible to allow cities to try radically different approaches and use an orchestration overlay to normalize them and provide a unified national view. In fact, it is very important to do so. As Ms. Neuman points out, "Comparing the rise of Smart Cities to similar Internet advancements, entirely homogenous solutions have lead to some of the largest compromises and least resilient solutions."

To net all this out, a software-centric orchestration system with distributed intelligence is the key enabler. In the software-centric world, the superscalers have a big head start. But they are burdened by a lack of trust and a lack of experience with widely geographically distributed nodes.

Thus, the telcos can capture this valuable market! To do so, they have to develop innovative software capability in orchestration and distributed intelligence. The current telco vendor ecosystem is not capable of providing this (see "Creating a Sustainable Innovation Ecosystem" from January, 2020). It is possible for Telco's to develop such a software driven innovation ecosystem (see "Software-Driven Ecosystems" from February 2020 and "Building an Innovation Ecosystem" from April 2020).

Capturing this opportunity will require change, and change is never easy. Yet change offers the only path forward in such a rapidly evolving world.